

# NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



## THESIS

### ENSURING A C2 LEVEL OF TRUST AND INTEROPERABILITY IN A NETWORKED WINDOWS NT ENVIRONMENT

by

Julie A. Lucas

September 1996

Thesis Advisor:

Gus Lott

Thesis Co-Advisors:

Cynthia E. Irvine

Rex Buddenberg

Approved for public release; distribution is unlimited.

19970103 025



| REPORT DOCUMENTATION PAGE  |  |   | Form Approved OMB No. 0704-0188  |
|--|--|---|----------------------------------|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.  |  |   |                                  |
| 1. AGENCY USE ONLY (Leave blank)   | 2. REPORT DATE<br>September 1996.                        | 3. REPORT TYPE AND DATES COVERED<br>Master's Thesis     |                                  |
| 4. TITLE AND SUBTITLE ENSURING A C2 LEVEL OF TRUST AND INTEROPERABILITY IN A NETWORKED WINDOWS NT ENVIRONMENT  |  | 5. FUNDING NUMBERS                                      |                                  |
| 6. AUTHOR(S) Lucas, Julie A.   |  |   |                                  |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Naval Postgraduate School<br>Monterey CA 93943-5000  |  | 8. PERFORMING ORGANIZATION REPORT NUMBER                |                                  |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)  |  | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER          |                                  |
| 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.   |  |   |                                  |
| 12a. DISTRIBUTION/AVAILABILITY STATEMENT<br>Approved for public release; distribution is unlimited.  |  | 12b. DISTRIBUTION CODE                                  |                                  |
| 13. ABSTRACT (maximum 200 words)<br>With the progression of computer systems to local and wide area networks, the scope of computer security has increased dramatically over the past two decades. Now, more than ever, the use of "trusted systems" is needed to ensure the secrecy, integrity, and availability of computer resources. However, attaining the levels of trust required has been difficult for a variety of reasons. This paper provides an in-depth look at the government's Trusted Computer System Evaluation Criteria (TCSEC) and its current applicability. An analysis of a military network running Windows NT version 3.51 as the network operating system is provided as a case study. The paper concludes with a discussion of the advantages and disadvantages of the TCSEC criterion. Although products have been certified as meeting the various class requirements, existing problems are preventing the attainment of "trusted" system from becoming a reality for many government organizations. |  |   |                                  |
| 14. SUBJECT TERMS Trusted Computer System Evaluation Criteria, TCSEC, Trusted Network Interpretation, TNI, Windows NT, Computer Security.  |  | 15. NUMBER OF PAGES 152                                 |                                  |
|  |  | 16. PRICE CODE  |                                  |
| 17. SECURITY CLASSIFICATION OF REPORT<br>Unclassified  | 18. SECURITY CLASSIFICATION OF THIS PAGE<br>Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT<br>Unclassified | 20. LIMITATION OF ABSTRACT<br>UL |



Approved for public release; distribution is unlimited.

**ENSURING A C2 LEVEL OF TRUST AND INTEROPERABILITY IN A  
NETWORKED WINDOWS NT ENVIRONMENT**

Julie A. Lucas  
Lieutenant, United States Navy  
B.S., Ohio State University, 1988

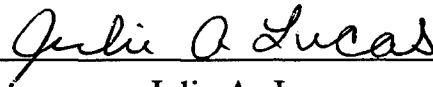
Submitted in partial fulfillment  
of the requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY  
MANAGEMENT**

from the

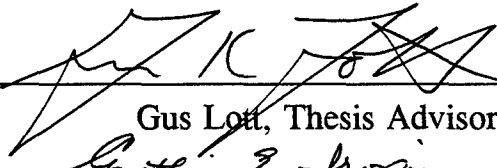
**NAVAL POSTGRADUATE SCHOOL  
September 1996**

Author:

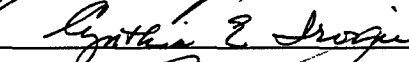


Julie A. Lucas

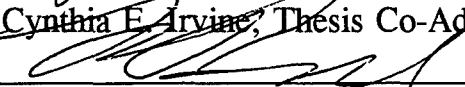
Approved by:



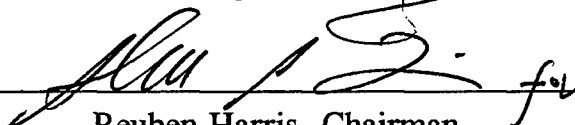
Gus Lott, Thesis Advisor



Cynthia E. Irvine, Thesis Co-Advisor



Rex Buddenberg, Thesis Co-Advisor



Reuben Harris, Chairman

Department of Systems Management



## **ABSTRACT**

With the progression of computer systems to local and wide area networks, the scope of computer security has increased dramatically over the past two decades. Now, more than ever, the use of "trusted systems" is needed to ensure the secrecy, integrity, and availability of computer resources. However, attaining the levels of trust required has been difficult for a variety of reasons. This paper provides an in-depth look at the government's Trusted Computer System Evaluation Criteria (TCSEC) and its current applicability. An analysis of a military network running Windows NT version 3.51 as the network operating system is provided as a case study. The paper concludes with a discussion of the advantages and disadvantages of the TCSEC criterion. Although products have been certified as meeting the various class requirements, existing problems are preventing the attainment of "trusted" system from becoming a reality for many government organizations.



## TABLE OF CONTENTS

|      |   |    |
|------|---|----|
| I.   | INTRODUCTION . . . . .  | 1  |
| A.   | PURPOSE . . . . .   | 1  |
| B.   | OBJECTIVE . . . . .   | 1  |
| C.   | RESEARCH QUESTIONS . . . . .  | 2  |
| D.   | SCOPE OF THE THESIS . . . . .                                       | 3  |
| E.   | RESEARCH METHODOLOGY . . . . .                                      | 3  |
| F.   | ORGANIZATION . . . . .  | 4  |
| II.  | COMPUTER SECURITY . . . . .   | 5  |
| A.   | GOALS OF COMPUTER SECURITY . . . . .                                | 7  |
| B.   | VULNERABILITIES AND THREATS . . . . .                               | 8  |
| C.   | ATTACKS ON COMPUTER NETWORKS . . . . .                              | 11 |
| D.   | COUNTERMEASURES . . . . .   | 13 |
| E.   | THE EVOLUTION OF GOVERNMENT COMPUTER SECURITY INITIATIVES . . . . . | 14 |
| III. | THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA . . . . .           | 21 |
| A.   | FUNDAMENTAL SECURITY REQUIREMENTS . . . . .                         | 22 |
| B.   | DIVISIONS OF TRUST . . . . .  | 24 |
| 1.   | Division D: Minimal Protection . . . . .                            | 24 |
| 2.   | Division C: Discretionary Protection . . . . .                      | 24 |
| 3.   | Division B: Mandatory Protection . . . . .                          | 25 |
| 4.   | Division A: Verified Protection . . . . .                           | 27 |
| C.   | ENSURING TRUST . . . . .  | 28 |
| 1.   | Trusted Computing Base (TCB) . . . . .                              | 29 |
| 2.   | Subjects and Objects . . . . .                                      | 30 |
| 3.   | Reference Monitor . . . . .   | 31 |
| 4.   | Bell and LaPadula Model . . . . .                                   | 32 |
| 5.   | Discretionary and Mandatory Access Control . . . . .                | 32 |
| 6.   | Protection Mechanisms . . . . .                                     | 34 |
| D.   | PRODUCT EVALUATION . . . . .  | 37 |
| E.   | CERTIFICATION AND ACCREDITATION . . . . .                           | 39 |
| 1.   | System Analysts . . . . .   | 41 |
| 2.   | Technical Analysis . . . . .  | 41 |
| 3.   | Risk Management . . . . .   | 44 |
| IV.  | THE TRUSTED NETWORK INTERPRETATION . . . . .                        | 47 |
| A.   | PART II SECURITY SERVICES . . . . .                                 | 49 |
| B.   | ENSURING TRUST . . . . .  | 52 |
| C.   | CERTIFICATION AND ACCREDITATION . . . . .                           | 53 |
| 1.   | Interconnected Accredited System View . . . . .                     | 53 |
| 2.   | Single Trusted System View . . . . .                                | 55 |
| V.   | THE FALCON LAN - APPLYING THE TCSEC/TNI CRITERION . . . . .         | 57 |
| A.   | SYSTEM FUNCTIONALITY AND GOALS . . . . .                            | 57 |
| B.   | SYSTEM CONFIGURATION . . . . .                                      | 59 |
| 1.   | Users . . . . .   | 59 |
| 2.   | Hardware . . . . .  | 61 |
| 3.   | Software . . . . .  | 63 |



|     |   |     |
|-----|---|-----|
| C.  | CLASS C2 REQUIREMENT . . . . .  | 64  |
| D.  | WINDOWS NT VERSION 3.51 OVERVIEW . . . . .  | 64  |
|     | 1. The Trusted Computing Base (TCB) . . . . .   | 66  |
|     | 2. Subjects . . . . .   | 72  |
|     | 3. Objects . . . . .  | 73  |
|     | 4. Object Access Rights . . . . .   | 75  |
|     | 5. Privileges . . . . .   | 77  |
|     | 6. File System Types . . . . .  | 78  |
|     | 7. C2Config.EXE . . . . .   | 78  |
| E.  | EVALUATING THE LEVEL OF TRUST . . . . .   | 81  |
|     | 1. Security Policy . . . . .  | 81  |
|     | 2. Accountability . . . . .   | 87  |
|     | 3. Assurance . . . . .  | 95  |
|     | 4. Documentation . . . . .  | 97  |
|     | 5. Additional TCSEC Features . . . . .  | 100 |
|     | 6. Other Security Services . . . . .  | 101 |
| F.  | MEETING INTEROPERABILITY REQUIREMENTS . . . . .   | 118 |
|     | 1. Provide a Communications System . . . . .  | 119 |
|     | 2. Provide a Student Tracking System . . . . .  | 120 |
|     | 3. Provide for Service Management . . . . .   | 120 |
|     | 4. Provide for Supply and Fiscal Tracking . . . . .   | 121 |
|     | 5. Provide Career Counseling Assistance . . . . .   | 121 |
|     | 6. Provide for Command Information<br>Dissemination . . . . .                                       | 122 |
|     | 7. Allow for the Sharing of Electronic mail with<br>DLI . . . . .                                   | 122 |
|     | 8. Provide for the Instruction of the Cryptologic<br>Technician Apprentice Common Core Curriculum . | 122 |
|     | 9. Provide for the Dissemination of Message<br>Traffic on the LAN . . . . .                         | 123 |
| VI. | CONCLUSION - THE PRO'S AND CON'S OF ENSURING TRUST . . .  | 125 |
| A.  | CONCLUSIONS . . . . .   | 125 |
| B.  | RECOMMENDATIONS . . . . .   | 126 |
| C.  | ADVANTAGES AND DISADVANTAGES OF THE TCSEC . . . . .   | 131 |
| D.  | SUMMARY . . . . .   | 134 |
|     | LIST OF REFERENCES . . . . .  | 135 |
|     | BIBLIOGRAPHY . . . . .  | 139 |
|     | INITIAL DISTRIBUTION LIST . . . . .   | 141 |

## I. INTRODUCTION

### A. PURPOSE

With the progression of computer systems to local and wide area networks, the scope of computer security has increased dramatically over the past two decades. The ability to adequately safeguard information while ensuring resource availability is becoming increasingly challenging to system administrators. Given enough time and resources, any system may be broken into and the information accessed. To prevent this occurrence, a balance must be achieved where the cost of breaking into the system outweighs the benefits derived from the action. The National Security Agency (NSA) developed the *Trusted Computer Systems Evaluation Criteria (TCSEC)* to provide those specifying a system with a set of expectations regarding the assurance of policy enforcement and to provide vendors with a set of standards against which systems could be developed. The purpose of this thesis is to analyze the TCSEC and its applicability to a Department of Defense (DOD) system in a networked environment using current technology.

### B. OBJECTIVE

The intent of this thesis is to examine the TCSEC and its application within the military using existing commercial products. During the past decade, much discussion has taken place within the DOD regarding the requirements for government computers to achieve specific levels of trust. At the beginning of the 1990's, "C2 by 92" was a phrase that was frequently used in computer meetings and

seminars throughout the DOD. However, the lack of available products, an overall lack of understanding of the technology and requirements, politics, and a lack of resources prevented that slogan from becoming a reality. Over the past few years, numerous vendors have been striving to furnish evaluated products which will now enable the Class C2 level of trust to be achieved.

With the continuing rise in the number of networks installed throughout the DOD and wider connectivity through the Internet, the importance of establishing a "trusted" system is rapidly gaining acceptance. A thorough analysis of the Class C2 certification process using a major network operating system such as Windows NT, is an excellent way to determine if the certification is attainable. Windows NT server was selected for this evaluation due to its increasing popularity among Navy commands.

### **C. RESEARCH QUESTIONS**

In order to achieve the objective listed above, the following research questions were addressed:

1. What are the requirements to achieve a Class C2 level of trust in a computer network?
  - a. How are computer networks certified for a specific level of trust?
  - b. What are the benefits of a "trusted" system?
  - c. What are the limitations of certification?
  - d. How does a Class C2 certification impact life cycle costs?
  - e. Can a network be connected to the Internet and still provide a Class C2 level of trust?

## 2. What are the capabilities of Windows NT Server 3.51?

- a. How does Windows NT support the Class C2 level of trust?
- b. What are the software's security limitations?
- c. How easily does Windows NT interface with other network systems?

### **D. SCOPE OF THE THESIS**

With computers and the information they maintain increasingly under attack, more people are beginning to take computer security seriously. However, many still do not fully understand what computer security is and why it is so important. This paper begins by identifying some basics of computer security. The TCSEC requirements are discussed in detail and an example application of the criterion is presented. In conjunction with the example application, an analysis of the Windows NT Server version 3.51 Network Operating System (NOS) is presented for both security and interoperability issues. Finally, the need for computer security standards for the government and the responsiveness of today's market to meeting those needs are addressed.

### **E. RESEARCH METHODOLOGY**

The primary methods of research to support this study included an in-depth literature search, use of the World Wide Web, and correspondence with government and industry representatives. The literature search included a review of numerous books, magazine articles, and government publications. The World Wide Web was used to obtain the latest information on the certification process and to gain information regarding the strengths and weaknesses of the

Windows NT software. Correspondence with officials at the National Security Agency (NSA), Microsoft, and other federal agencies were used to obtain information on test results, computer security problems, and future actions.

## **F. ORGANIZATION**

The remainder of this thesis is organized as follows:

- Chapter II, "Computer Security," provides a general overview of computer security. The goals of computer security are discussed and security terms are defined. The chapter concludes with a brief description of the evolution of government computer security initiatives.
- Chapter III, "The Trusted Computer System Evaluation Criteria (TCSEC)," identifies the fundamental security requirements upon which the evaluation criterion are based. The divisions of trust and terminology used with the criterion are discussed in detail. The system certification and accreditation process is described. In addition, the product evaluation process is briefly described.
- Chapter IV, "The Trusted Network Interpretation (TNI)," compares the criterion for a network evaluation to the stand-alone TCSEC criterion. The differences in the evaluation processes are briefly described.
- Chapter V, "The Falcon LAN - Applying the TCSEC/TNI Criterion," presents an overview of the network installed at the Defense Language Institute and provides an in-depth analysis of Windows NT 3.51 server. Both trust and interoperability issues are discussed.
- Chapter VI, "Conclusion - The Pro's and Con's of Ensuring Trust," discusses the benefits and pitfalls of applying the TCSEC to military systems today. Issues such as the effect on system life cycle costs, the time required for product evaluation, and the market's responsiveness to providing trusted products are presented. A summary of research findings and recommendations for ensuring the DLI LAN is included.

## II. COMPUTER SECURITY

With today's expanded availability of computers, an increasing number of people are finding themselves vulnerable to the perils of the information age. As such, the topic of computer security is becoming a "hot issue." Computer security isn't a new topic, but one that has existed since the development of the first computer. What is new, however, is the broader view that must be taken to ensure the security of a system and the information it contains.

Government agencies are particularly vulnerable to computer intrusions due to the nature of the business conducted and the high profile target they represent. Since the late 1980's, several attacks or intrusions have become well publicized. For example, the West German Computer Club (better known as the Chaos Club) announced in 1987 that it had successfully penetrated NASA's computer systems. NASA was unaware of this intrusion until messages began appearing on their system. Also in 1987, a 75 cent accounting error alerted Cliff Stoll, an astronomer turned systems manager at Lawrence Berkeley Lab, to another intrusion. For two years, Dr. Stoll followed the intruder as he tried to break into over 450 computer systems (many of which were government owned). [Ref. 1] Eventually the chase led to a small group of West German hackers with ties to the Soviet KGB. Finally, the computer worm of 1988 was released on the Internet by Robert T. Morris, Jr., a Cornell University graduate student, on November 2nd. In less than 48 hours, the worm spread throughout the network, infecting more than 2,100 computers. Although no data was actually destroyed, the

cost of fixing the systems and lost work hours was estimated at over \$1 million. [Ref. 2] These are just a few examples of where the absence of secure systems and computer security management techniques have resulted in serious intrusions and why improved approaches to computer security are required.

The government is not alone with respect to this need. With the rapid increase in the number of computer systems, computer crime has become a major threat to American business. "According to the Federal Bureau of Investigation (FBI), computer crime is currently the most expensive form of commercial crime - with an average cost of \$450,000 per theft. This represents a greater risk to corporations than fire or any other type of hazard." [Ref. 3: p. 7] In addition, the FBI estimates the total figure for computer theft may range as high as \$5 billion per year. Compounding the problem is the lack of law enforcement attention given to these crimes. Estimates indicate that up to 90% of all computer crimes and intrusions are never reported outside of the organization. Of those that are reported, only a fraction of the cases are ever prosecuted. [Ref. 3: p. 8] In fact, reports concerning computer crime date back to the 1940's. However, it wasn't until 1966 that the first federal prosecution for a computer crime took place. The case involved the use of a computer to alter the records of a Minneapolis bank. [Ref. 4: p. 16]

There are several reasons why computer security breaches are not publicized. Government system intrusions are not publicized in an attempt to limit the disclosure of security holes or

vulnerabilities. By publicizing such information, other computer intruders may take advantage of the information gained to penetrate additional government systems with the same or similar weaknesses.

In the commercial sector, computer intrusions are not publicized for fear that customers would lose confidence in a company and take their business elsewhere. Legal concerns also keep many businesses from publicizing computer intrusions. If a company maintains information on customers or employees that is protected under the Privacy Act of 1987, the company may be held liable for any unauthorized disclosure of the information. This liability could further increase any financial losses caused by the intrusion.

The use of "trusted" computer systems is one approach to dealing with problems such as these. However, before discussing the criterion used to achieve trust in a system, an overview of computer security and its terminology is needed. The following sections present this overview. Although not every aspect of computer security is presented here, the reader should achieve a good basic understanding of what computer security is and what threats it is trying to avoid.

#### **A. GOALS OF COMPUTER SECURITY**

Computer security focuses on the achievement of three main goals: secrecy (confidentiality), integrity, and availability. Secrecy ensures information including unclassified, private, sensitive, and classified data, is not disclosed to an unauthorized



person. Integrity, also referred to as accuracy, means the system must not corrupt the information maintained on it or permit any unauthorized changes to occur through either accidental or malicious means. Availability ensures the system is operating efficiently and is able to recover quickly and completely in the event of a disaster or attempted disruption. Loss of power, flooding, fire, and unwelcomed system penetration are all examples of disasters for which a system must be prepared. If users are unable to access the computer resources needed, then a denial of service has occurred.

In addition to these goals, computer networks have introduced two additional requirements: authentication and nonrepudiation. Authentication requires the address of a message (such as electronic mail) to be identified with a high level of certainty that the address is correct. In a sense, it is an aspect of integrity. Nonrepudiation implies that neither the sender nor receiver of a message can deny its transmission.

Achievement of any or all of these goals is dependent upon the environment in which the system is operating. In some cases, one or two aspects of security may be more important than the others. To determine the services which are needed, the goals and environment of each computer system must be assessed.

## **B. VULNERABILITIES AND THREATS**

A security assessment typically identifies the vulnerabilities and threats to a system. A vulnerability indicates a point where

a system is susceptible to an attack. Examples of system vulnerabilities include: physical threats, natural disasters, mechanical breakdowns, electronic signals, external connections, and people. If the computer system is a network, it is vulnerable at any point where it contacts another network or system. Vulnerable points include bridges, routers, and modems, as well as floppy diskettes and portable computers.

A threat is an avenue through which a person or event may exploit a vulnerability to adversely affect the system. Security experts list toll fraud, theft, viruses, disgruntled employees, accidents, and ignorance as the most likely threats faced by system administrators today. [Ref. 4: p 9] In terms of numbers, errors and accidents typically represent the largest threat to a network. As Richard Baker noted in his book Network Security: How to Plan for it and Achieve It:

One of the biggest obstacles to effective computer security today is an epidemic of misplaced emphasis. Corporations spend a lot of time and money buying and installing elaborate computer security systems to protect themselves from well-publicized outsiders like youthful invaders and virus carriers. They do next to nothing to train employees to make regular backups or to avoid that stereotype of computer insecurity: the password on a sticky note attached to the monitor. By one estimate - really a guess, but a reasonable one - system administrators who accidentally destroy data by punching the wrong key outnumber crazed hackers by at least 10 to 1. [Ref. 4]

Lack of training is not the only threat from the users of a system. It is estimated "that as many as 80 percent of system penetrations are conducted by fully authorized users who abuse

their access privileges to perform unauthorized functions." [Ref. 3: p. 16] The Justice Department conducted an analysis of computer abuse cases and identified the following functions as the points where data processing systems tended to be the most vulnerable: [Ref. 4]

- Poor controls over data handling
- Weak or missing physical controls
- Inadequate procedural controls
- Weak ethical standards
- Poor programming practices
- Operating system weaknesses
- Lack of user identification
- Inadequate control over storage media

A "newspaper effect" within some organizations causes many system administrators to focus on the highly publicized external threats such as hackers and viruses. As a result, too little attention is given to basic countermeasures such as backups and passwords, which can prevent more serious problems from within the organization.

Networks in particular, suffer from an additional weakness caused by system administrators focusing on the end system and not the network as a whole. For example, many network administrators expend much effort and resources to protect the hosts on the network, yet pay little or no attention to the overall network. This is because it is generally easier to protect the hosts rather

than the entire network, and intruders are more likely to go after the data on the host. However, there are sound reasons for protecting the overall network. By focusing on the host alone, the entire network may be subject to vulnerabilities that are overlooked. For example, an intruder may be able to divert transmitted data to an off-site host for examination or to search for passwords. Human error, in the form of a misconfigured host could lead to a degradation in service for network users. Or, a denial of service attack may be generated without the attacker ever penetrating the system. By focusing on the entire network, vulnerabilities such as these should be identified.

### **C.    ATTACKS ON COMPUTER NETWORKS**

Attacks on a computer network may be passive or active. Passive attacks include eavesdropping and monitoring transmissions to gather information. The information may be gained either directly from the contents of a message or indirectly through traffic analysis. Traffic analysis is a more subtle form of passive attack, but one which should not be neglected when securing a system. Usually passive attacks are difficult to detect since information is not changed in any way. Most security techniques to guard against such attacks are preventive in nature rather than geared toward detection.

Unlike passive attacks, active attacks involve the modification of information or the insertion of false information.

Active attacks are typically divided into four main categories: masquerade, replay, modification, and denial of service.

- A masquerade occurs when one person or group pretends to be someone else. (A masquerade normally includes another form of active attack as well.)
- A replay occurs when the contents of a message is captured and then retransmitted to produce an unauthorized effect.
- If part of a legitimate message is altered, delayed, or reordered, then a modification attack has taken place. The modification category also includes attacks by malicious software which alter the contents of a file.
- If the normal use or management of a system is prevented or constrained in any way, then a denial of service attack has been implemented. A denial of service attack can also result from the introduction of malicious software which consumes system resources.

Unlike passive attacks, active attacks are generally difficult to prevent. The goal in dealing with active attacks is normally to detect them and then recover from any disruption or delays they may have caused.

Using the three main goals of computer security (secrecy, integrity, and availability), attacks on computer systems fall under four main categories: interruption, interception, modification, and fabrication. [Ref. 2: pp. 7-8]

- Interruption is an attack on the availability of a system in which part of the system is either destroyed or becomes unavailable.
- Interception occurs when an unauthorized entity gains access to the system, attacking the system's confidentiality.

- If an unauthorized person gains access and tampers with the system or the information it maintains, then a modification has occurred and the system's integrity has been attacked.
- A fabrication has occurred if an unauthorized user inserts false information into the system, affecting its authenticity.

#### **D. COUNTERMEASURES**

Once the vulnerabilities and threats to a system have been determined, specific countermeasures to prevent or recover from the effects of these risks must be implemented. There are numerous types of countermeasures available. Computer security countermeasures focus on the operating system features which control access to a system, and communications security measures are used to protect transmitted information. Countermeasures associated with communications security are used on computer networks to control access to the network computers from both internal and external connections. Finally, physical security countermeasures are used to protect a computer system from natural disasters and intruders. Typically, countermeasures of all three forms will be required for most computer systems.

"It is anticipated that by the year 2000, information will account for a larger portion of the U.S. gross national product than manufactured products and other physical commodities." [Ref. 1] With this increased reliance on information, the security mechanisms required to ensure the confidentiality, integrity, and availability of the information must be widely implemented.

Driving these security requirements is the U.S. government. Each year, the government classifies approximately 6.8 billion pieces of information which must be protected. [Ref. 3: p. 18] To ensure the information is protected uniformly throughout the government, standards were required. The development of standards began in 1965 with the passing of the Brooks Act. Since then, numerous government efforts have been aimed at achieving a uniform management of federal Information Technology (IT) resources. As a result, a foundation has been formed over the past 30 years for all aspects of IT management.

#### **E. THE EVOLUTION OF GOVERNMENT COMPUTER SECURITY INITIATIVES**

Computer security efforts began in the 1950's when the first TEMPEST security standard was developed. TEMPEST refers to "technology that shields computer equipment to keep electromagnetic emissions from being intercepted and deciphered by eavesdroppers." [Ref. 3: p. 17] Also during the 1950's the U.S. Communications Security (COMSEC) Board was established. Composed of representatives from various branches of the government, COMSEC was given the oversight responsibility for protecting classified information. In addition, some early system designs were developed with security features built-in.

It wasn't until the 1960's, however, that public awareness was raised concerning computer security. During that decade, numerous initiatives were started by the Department of Defense (DOD), the

National Security Agency (NSA), and the National Bureau of Standards (NBS). Specifically:

- The Automatic Data Processing Equipment Act (better known as the Brooks Act) was passed by Congress in 1965. As a consequence of this act, the NBS was placed in charge of researching and developing standards for the procurement and use of federal computer systems. Initially, NBS efforts were focused on evaluating the existing systems and studying the government's computer security requirements. During the 1970's, NBS efforts shifted to developing computer security standards in two distinct areas: building and evaluating secure systems and cryptography. Several seminars and workshops were held to define the problems facing federal computer systems and to develop solutions to these problems. As a result, numerous reports were generated with the conclusion that computer security required attention in three areas: policy, mechanisms, and assurance. Policy was needed to state the security rules required to ensure the security of sensitive information. Hardware and software mechanisms would be used to enforce the policy, and the enforcement should provide a reasonable level of assurance that the policy was supported even when a computer system was subjected to threats.
- To develop the policy, mechanisms, and required assurance proposed by the NBS efforts, three specific actions were recommended. First, a detailed computer security policy for sensitive information was needed. Second, a formal security evaluation and accreditation process was required that would include the publication of a list of approved products for handling sensitive information; and third, a standard, formalized technical means of evaluating the overall security of a system was needed. The task of developing an initial set of computer security evaluation criterion was assigned to the Mitre Corporation. To fulfill the other tasks, the Office of the Secretary of Defense sponsored several public seminars. As a result of the seminars, the NSA was placed in charge of increasing the use of trusted information security products within DOD.
- In 1967, DOD assembled a task force within the Advanced Research Project Agency (ARPA) to study the potential threats to DOD computer systems and information. The task force worked for two years examining computer systems and networks, identifying vulnerabilities and threats, and establishing methods for protecting and controlling access to government computers and information. In 1970, the task



force published its report, *Security Controls for Computer Systems*, which has been viewed by many as a landmark publication in the history of computer security. [Ref. 3: p. 28] The research that followed this report led to numerous programs aimed at protecting classified information and setting computer security standards. In 1972, a directive and an accompanying manual was issued by DOD establishing a consistent policy for computer controls and techniques.

The initiatives started during the 1960's continued into the 1970's. Government and industry sponsored "tiger teams" were organized to attempt to break into computer systems in order to find security holes and then correct them. The teams were effective at finding numerous security gaps. However, it soon became apparent that the only means of "guaranteeing" system security was to design verifiable protection mechanisms into the systems from the beginning.

In addition to the tiger teams, a number of research projects aimed at identifying security requirements, formulating security policy models, and defining recommended guidelines and controls were initiated. As a result, several concepts and reports were produced. For example, the concept of a reference monitor was introduced by James P. Anderson. The reference monitor is used to "enforce the authorized access relationship between subjects and objects of a system." [Ref. 3: p. 30] Also during the 1970's, David Bell and Leonard LaPadula developed the first mathematical model of DOD security policy which has become known as the Bell and LaPadula model. Both the reference monitor concept and the Bell and LaPadula model were included in later government computer security standards.

Most of the government efforts aimed at developing a secure system during the 1970's were pointed toward the formation of a security kernel. The kernel is part of the operating system which controls access to system resources. An initiative funded by the Air Force eventually led to the development of security mechanisms for the Multiplexed Information and Computing Service (MULTICS) system. MULTICS was a large-scale, highly interactive system that offered both hardware and software security features. Users with different security clearances could simultaneously access different levels of classified information. MULTICS was extremely important because it provided the foundation for the later development of other secure systems.

In an attempt to focus national attention and resources on computer security, the DOD Computer Security Initiative was announced in 1977. Under this initiative, a series of seminars were held with participants from both government and industry addressing the following questions: [Ref. 3: p. 32]

- Are secure computer systems useful and feasible?
- What mechanisms should be developed to evaluate and approve secure computer systems?
- How can computer vendors be encouraged to develop secure computer systems?

To expand upon the work completed under the DOD Computer Security Initiative, NSA created the DOD Computer Security Center (CSC) on 2 January 1981. During the following years, the role of the CSC was modified to encompass all federal systems and the name

changed to the National Computer Security Center (NCSC) in August 1985. The center's role since its beginning has been to evaluate and promote the use of trusted systems in the federal government. As such, the NCSC has played a vital role in the field of computer security over the years.

In August 1983, the NCSC published the *Trusted Computer System Evaluation Criteria (TCSEC)*, also known as the Orange Book. The publication was based on the criterion developed by the Mitre Corporation and other earlier security developments such as the Bell-Lapadula Model. [Ref. 3: p. 35] Since its publication, the TCSEC has become "the Bible of secure system development," describing the criterion used to assess the level of trust that can be placed on a particular computer system. Products are submitted to the NCSC by vendors requesting an evaluation for a specified level of trust. Upon the successful completion of the evaluation process, the products are added to the center's Evaluated Products List.

Since the issuance of the TCSEC, NCSC has also provided a series of additional publications which are used to interpret various aspects of the criterion including network communications, security subsystems, and specialty products. These publications are referred to as the Rainbow Series.

The field of computer security has continued to develop since the publication of the TCSEC. However, since the focus of this thesis deals with the TCSEC and its application today, the

discussion of computer security developments will stop at this point so the TCSEC can be discussed in further detail.



### III. THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

The *Trusted Computer System Evaluation Criteria (TCSEC)*, or Orange Book, was first published by the National Computer Security Center (NCSC) in August 1983. In 1985, the original publication was revised slightly and reissued in December. Since its initial publication, the TCSEC has provided the ground rules for evaluating the level of trust that can be given to a specific computer system. As Russell and Gangemi state in Computer Security Basics, the TCSEC "effectively makes security a measurable commodity so a buyer can identify the exact level of security required for a particular system, application, or environment." [Ref. 3]

The TCSEC measures trust through two perspectives - security policy and assurance. Security policy provides the rules that are to be enforced by a system's security features. Assurance refers to the trust that can be placed in a system, and includes the methods used to "prove" the security features have been developed, tested, documented, maintained, and delivered to a customer. At the lower levels, assurance is gained mostly through the testing of the system. At the higher levels, assurance is derived more from a rigorous approach to system design and implementation.

The TCSEC defines four broad divisions of security protection which, in increasing order, are: D - Minimal Security, C - Discretionary Protection, B - Mandatory Protection, and A - Verified Protection. Each division is further refined into one or more numbered classes. The higher the number, the greater the level of protection afforded within the division.

Each class is defined by a specific set of criterion that must be met to be awarded the rating of that class. The criteria fall into four main categories: security policy, accountability, assurance, and documentation. The levels of trust are cumulative with each building upon the requirements of lower classes. A brief description of each division is provided in section B of this chapter.

#### **A. FUNDAMENTAL SECURITY REQUIREMENTS**

The TCSEC dictates that trusted systems will control access to all information through the use of specific security features. These features must ensure that only authorized users (or processes operating on behalf of the users) will have access to the information. Furthermore, the access permitted will be based on the capabilities (i.e., read, write, create, delete) that have been authorized for the user. To ensure the security, six fundamental requirements were created: [Ref. 5: pp. 3-4]

- **Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system.** Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information. These rules include requirements such as: No person lacking proper personnel security clearance shall obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know).

- **Requirement 2 - MARKING - Access control labels must be associated with objects.** In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g., classification), and/or the modes of access accorded those subjects who may potentially access the object.
  
- **Requirement 3 - IDENTIFICATION - Individual subjects must be identified.** Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system.
  
- **Requirement 4 - ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.** A trusted system must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.
  
- **Requirement 5 - ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above.** In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.
  
- **Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes.** No computer system can be considered truly secure



if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer system's life-cycle.

Requirements 1 and 2 deal with a system's policy, 3 and 4 reflect the system's accountability, and 5 and 6 deal with the level of assurance offered by a system. It was from these six requirements that the actual evaluation criterion were derived.

## **B. DIVISIONS OF TRUST**

### **1. Division D: Minimal Protection**

Division D contains only one class and is reserved for those systems which fail to meet a higher assurance level. Given the amount of time and money required for a vendor to submit a system for evaluation, systems are normally not submitted for this rating. However, if a system fails to meet the Class C1 requirements, it may receive a Class D rating.

### **2. Division C: Discretionary Protection**

Division C consists of two classes, C1 and C2. Systems certified at this division of trust must provide discretionary or need-to-know protection as well as audit capabilities. The design of a Trusted Computing Base (TCB) is central to systems evaluated at this level and higher. The TCB provides a separation of users and data so the access controls may be implemented.

Class C1 systems provide discretionary security protection by providing a separation between users and data. The environment in which a C1 system is used is expected to be one of cooperation with

users processing data at the same level of sensitivity. At the C1 level, users are permitted to log into the system as a group, using a shared password.

Class C2 is referred to as the Controlled Access Protection class. Systems certified at this level provide access control that is granularized to the individual user. Login procedures, auditing capabilities, and resource isolation all hold users individually accountable for their actions. In a Class C2 environment, each user must log into the system using a unique password or identifier. Shared passwords are not permitted. In addition, object reuse features must be present to prevent the unauthorized disclosure of information.

### **3. Division B: Mandatory Protection**

The TCB is used to maintain the integrity of sensitivity labels which are used to enforce a set of mandatory access control rules. The sensitivity labels must be used with all major data structures in the system. As part of the product evaluation, the system developer must provide the security policy model and specifications on which the TCB is based. In addition, it must be clear that the reference monitor concept was used in the design of the system.

The B division consists of three separate classes. Class B1 introduces Mandatory Access Control (MAC) through the addition of labels. An informal statement of the security policy model, data labeling, and MAC for named subjects and objects must be included

in the system design. Sensitivity labeling must also be provided for all exported information.

The differences between Classes C2 and B1 protection are minimal. Theodore M.P. Lee presents an interesting analysis of these ratings for systems operating in compartmented mode. With compartmented mode, some system users are not formally authorized access to all of the information maintained on the system. In his paper *"A Note on Compartmented Mode: To B2 or not B2?"*, Mr. Lee recommends a rating of B2 or higher for compartmented mode systems. [Ref. 6]

Class B2 provides structured protection by building on the capabilities provided in Class B1. Class B2 is the first level where the reference monitor concept is substantially implemented into the system design. The TCB must be based on a clearly defined and documented formal security model that provides both discretionary and mandatory access control to all levels of the system. The TCB is carefully structured into protection-critical and non-protection-critical elements with a well defined interface. The system must be relatively resistant to penetration and covert channels must be addressed. Products submitted for evaluation at this level are subjected to a more thorough test and review than those submitted for lower classifications.

Class B3 provides security domains with the reference monitor concept fully enforced. The system must be designed with complexity minimized and non-essential code excluded. Support is provided to the system administrator through expanded auditing

capabilities and system recovery procedures. The search for covert channels is also expanded to include both storage and timing channels. Should a system failure occur, trusted recovery features must be implemented to ensure the recovery of resources without a compromise of data. Finally, more extensive documentation of the system security features is required for a Class B3 evaluation.

#### **4. Division A: Verified Protection**

Formal security verification methods are used to ensure the system's mandatory and discretionary access controls will effectively protect classified and sensitive information. This level requires extensive documentation to be submitted during the evaluation process. Class A1, verified design, is the only class currently listed in this division. Functionally, the requirements for A1 are equivalent to those for a B3 certification, with the addition of trusted distribution. Trusted distribution provides control over the integrity of the data describing the TCB. Procedures must be implemented to ensure any data updates distributed to customers precisely match the master copies.

The main difference between the B3 and A1 classes results from the analysis and verification techniques used on the formal design. The techniques result in a higher level of assurance that the TCB is correctly implemented. In addition, more stringent configuration management is required.

### C. ENSURING TRUST

Given enough time and resources, any computer system can be penetrated or subverted regardless of the trust engineering and security features that are provided. Therefore, the TCSEC measures the level of trust that can be provided by a system to ensure the system will enforce the security policy over time. The TCSEC defines a trusted system as one "that employs sufficient hardware and software integrity measures to allow its use to simultaneously process a range of sensitive unclassified or classified (e.g., confidential through top secret) information for a diverse set of users without violating access privileges." [Ref. 5] "Inherent to the concept of trust is some assurance that the trusted person or entity possesses the required strength, capability, and integrity to merit that trust." [Ref. 7: p. 13] The trust is actually built from the bottom or hardware level up, with each layer "trusting" the lower layers to perform

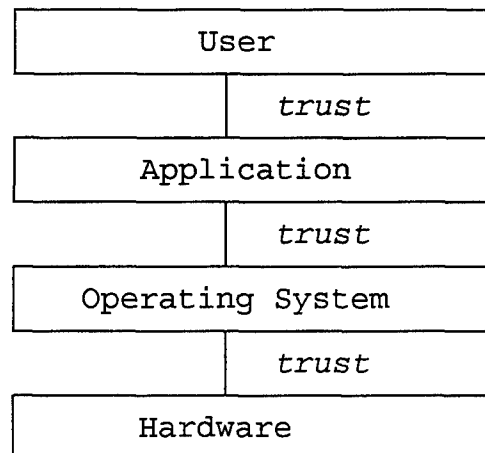


Figure 1: Trust Hierarchy in a Computer System [Ref 7]

their services reliably and accurately. Figure 1 was taken from NCSC's *Assessing Controlled Access Protection* [Ref. 7] and describes this layering of trust graphically.

Several different concepts are used in order to achieve these various levels of trust. The following sections provide a brief synopsis of the major concepts used throughout the TCSEC.

### **1. Trusted Computing Base (TCB)**

Central to the idea of a trusted system is the concept of a Trusted Computing Base (TCB). The TCB is used to refer to the mechanisms that enforce a system's security and is defined as:

The totality of protection mechanisms within a computer system - including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy. [Ref. 5]

Normally the TCB does not include the entire system. Part of the analysis of any product submitted for evaluation is the identification of the TCB (i.e., the architecture, assurance mechanisms, and security features that work together to form the TCB). Once identified, the TCB is evaluated to determine how well it is protected from tampering and interference.

The size and structure of the TCB will vary across the different classes of trust. At the Class C2 level, the TCB will normally be large, dispersed, and unstructured. This presents a

challenge to both evaluators and system administrators for assuring and maintaining the system's security. As a system progresses up the trust hierarchy, the TCB typically becomes smaller and more structured. At the B2 level, the TCB may still be large. However, due to increased structure in the software engineering designs and use of hardware protection features, the modularity increases, resulting in a system that is easier to understand, evaluate, and maintain. Finally, systems meeting the B3 and A1 levels of trust generally have TCB's which are small, layered, and highly structured permitting more rigorous testing and evaluation to be conducted.

## **2. Subjects and Objects**

The terms subjects and objects are typically used to refer to the entities of a computer system. Subjects are active entities such as people, processes, or devices, which can cause information to flow within the system or can cause the state of the system to change.

Objects are passive devices that contain or receive information. Files, directories, directory trees, records, segments, printers, network nodes, clocks, keyboards, and processors are all examples of objects. Access to an object is associated to a subject through a right or access mode. When a subject is authorized access to an object, access is also authorized to the information contained in the object. The set of objects that a subject is able to access is referred to as the subject's domain.

### 3. Reference Monitor

The reference monitor is used to enforce "the authorized access relationships between subjects and objects of a system." [Ref. 3: p. 107] The reference monitor serves as an interface between a subject and the object to which the subject seeks access. When a request is made, the reference monitor accepts the request, consults the appropriate access control information, and then permits or denies access to the object accordingly. Any reference to an object must be validated against the access control information, even if it is a reference by another program.

The mechanism used to implement the reference monitor in a system must meet three design requirements: isolation, completeness, and verifiability. Isolation means the mechanism must be tamper proof. To achieve completeness, the monitor must be used for every access decision without being bypassed, and the monitor must be capable of being analyzed and tested for verification.

The security kernel is the operating system mechanism that is normally used to implement the reference monitor concept. As such, it supervises all system activity in accordance with the system's security policy. In following with the design principles outlined above, the TCSEC dictates that the security kernel "must mediate all access, be protected from modification, and be verifiable as correct." [Ref. 5] The security kernel is typically viewed as the heart of the TCB. (Note: the reference monitor concept does not apply to a Class C2 system.)



#### 4. Bell and LaPadula Model

Models are used to precisely express a system's security requirements. All mechanisms used to support the security policy must conform to the selected model for the system. The Bell and LaPadula model was the first mathematical model for DOD security policy and was the model selected for use with the TCSEC. The model provides a formal description of the paths over which information is allowed to flow in a secure system and applies strictly to the secrecy of the information. The paths are important since they describe acceptable relationships between subjects and objects at different levels of sensitivity. The following provides the details of the model:

Each system covers a set of subjects  $S$  and a set of objects  $O$ . For each subject  $s$  in  $S$  and each object  $o$  in  $O$  there is a fixed security class  $C(s)$  and  $C(o)$ . The security classes are ordered by a relation  $\leq$ .

Two properties characterize the secure flow of information:

**Simple Security Property:** A subject  $s$  may have read access to an object  $o$  only if  $C(o) \leq C(s)$ .

**\*-Property:** A subject  $s$  who has read access to an object  $o$  may have write access to an object  $p$  only if  $C(o) \leq C(p)$ .  
[Ref. 8: pp. 249-250]

#### 5. Discretionary and Mandatory Access Control

The features of a computer system which enable access to an object to be restricted are referred to as access control mechanisms. The controls may be implemented through hardware or software features, operating procedures, or management procedures. If access is restricted based upon the identity of the user or

group of users, then a Discretionary Access Control (DAC) policy is used. Under a DAC policy, an authorized user is capable of passing permissions to another user. For example, one user can share a file with another user and permit him/her to modify the file.

In contrast, Mandatory Access Control (MAC) provides a stricter policy than DAC. Under a MAC policy, access to system objects is restricted according to the sensitivity of the information contained in the object and the authorization level of the subject to access that information. The sensitivity of the information is represented by a security level associated with the object, and the subject's authorization level is normally represented by a clearance. Under a strictly MAC policy, users are not permitted to share files or to pass permissions to other users.

Any access control policy is either mandatory or discretionary. The policy is a "MAC policy if, and only if, it can be represented by a partially ordered set of access classes; otherwise, it is discretionary." [Ref. 9] A key distinction between the two forms is the level of protection provided against malicious software. For example, a Trojan Horse can bypass DAC controls, but cannot bypass the controls of a MAC policy. This can be demonstrated through mathematical algorithms. Specifically, with a DAC policy, an algorithm which determines whether an arbitrary protection system will ever result in unauthorized access to information cannot be devised. [Ref. 10] However, with a MAC policy, it is possible to construct a lattice of access classes and mathematically prove that access control is always enforced.

## 6. Protection Mechanisms

Mechanisms are functional features of a computer system which are designed to enforce the security policy and accountability objectives. The mechanisms addressed by the TCSEC include: identification and authentication, Discretionary Access Control (DAC), object reuse, and audit capabilities. [Ref. 7: p. 22]

Identification and authentication is normally achieved by asking for a login name followed by a prompt for some sort of "proof" that the user is in fact the person to which the login name is assigned. The login name achieves the identification and the "proof" is used for authentication. Three types of "proof" are used for most systems: "(1) something the user knows (e.g., a password); (2) something the user has (e.g., an authentication device); or (3) something the user is (e.g., a retinal scan)." [Ref. 7: p. 23] Most products on the Evaluated Products List (EPL) use the login name and password combination to accomplish identification and authentication.

The DAC mechanism is used to restrict access to objects based upon the identity of a subject. Access Control Lists (ACLs), protection bits, capabilities, profiles, and passwords are the main mechanisms used to implement DAC. ACLs are associated with objects and identify subjects with authorized access as well as the type of access granted. Protection bits identify access privileges through a bit vector, with each bit representing a different type of access (e.g., read, write, etc.). The protection bits may be assigned according to specific categories of users (e.g., owner,

group, public) to implicitly associate access rights with individual users. Capabilities may be assigned to a user for protected objects with access being granted to a subject only if he or she has the appropriate capability. Profiles associate a listing of protected objects to each user which identifies the objects to which the subject has been granted access. Finally, passwords may be used to permit full (all types) or partial (different types such as read only) access to objects.

Despite the specific mechanism used to implement DAC within a computer system, all DAC implementations are susceptible to attack by a Trojan Horse. Specifically, when a DAC program executes, it uses the access privileges of the user initiating the program. A Trojan Horse will utilize these permissions to pass or modify information in a manner not intended by the user. If separating classified information is left to the user's discretion, then a Trojan Horse can result in an unauthorized disclosure of information. Therefore, DAC mechanisms are not sufficient for segregating objects with different classification levels. *A Guide to Understanding Discretionary Access Control in Trusted Systems* provides a more detailed description of the Trojan Horse problem.

[Ref. 11: pp. 5-6]

Object reuse provides assurance that information is not available to other users once storage space has been reallocated. Table 1 was taken from NCSC's *Assessing Controlled Access Protection* document and outlines the various object reuse mechanisms for the various types of storage objects.

The audit criterion requires that the computer system be capable of collecting information regarding system events. The audit features provide a record of security related events which may be examined either as the events are occurring or retrospectively. Once the audit mechanism collects the event data,

| Storage Object   | Implementation   |
|--|--|
| Primary Storage<br>(e.g., random access memory, cache, translation buffer) | - Overwriting memory page with fixed or random pattern and/or (for efficiency) new data  |
| Fixed Media<br>(e.g., fixed disk, terminal, operator console)              | - Overwriting physical data blocks<br>- Purging associated entries in page management table<br>- Purging directory information residing on media |
| Removable Media  | - On-line overwriting with approved fixed or random pattern<br>- Degaussing<br>- Off-line overwriting  |

Table 1. Object Reuse Mechanisms [Ref 7]

the TCB must protect it from unauthorized modification or destruction. At a minimum, the audit mechanism must be able to record the following types of events: [Ref 7: p. 31]

- System logins
- Introduction of objects into a user's address space (e.g., file open, file creation, program execution, file copy)
- Deletion of objects from a user's address space (e.g., file close, completion of program execution, file deletion)
- Actions taken by system administrators and/or system security personnel (e.g., adding a user)

- All security relevant events (e.g., use of privileges, changes to DAC parameters)
- Print requests

In addition to the type of event recorded, the audit mechanism must identify the time and date of the event, the origin of the request, whether it was a success or failure, and provide a unique identifier representing the subject who requested or "supposedly" requested the event. If the event is the introduction or deletion of an object to a user's address space, then the name of the object must be recorded. Finally, any actions taken by the system administrator must be described in the audit trail.

#### **D. PRODUCT EVALUATION**

The National Computer Security Center (NCSC) evaluates operating systems and other products according to the criterion set forth in the TCSEC through the Trusted Product Evaluation Program (TPEP). TPEP is the primary program of the NCSC and is aimed specifically at Commercial Off-The-Shelf (COTS) products which meet the needs of the government. To be certified at a specific level of trust, the product and vendor must complete both a preliminary product evaluation and a formal product evaluation. Once a product is assigned a specific rating, it is placed on the Evaluated Products List with its assigned rating. The Rating Maintenance Program (RAMP) allows for technological advancements, by permitting software changes and new hardware platforms to be added to the evaluated package.

It is important to remember that although a system is assigned a specific rating, that rating pertains only to the hardware platform on which the testing was completed. Therefore, if an operating system was assigned a Class C2 rating on a Compaq Proliant 2000 without floppy drives, the Class C2 rating would not be transferrable to a different platform such as a Gateway 2000 P5-120 with floppy drives. In addition, products evaluated according to the TCSEC do not maintain that rating when used in a networked environment. The TCSEC focuses strictly on stand-alone systems which are not interconnected with other systems.

As the number of computer networks continues to grow, the need for products evaluated for a networked environment is rapidly increasing. Evaluations for networked products follow an expanded testing process based upon the *Trusted Network Interpretation (TNI)* or Red Book. (The TNI will be discussed in further detail in the next chapter.) The evaluation process used to assess the security characteristics of a product in a networked environment is referred to as the TPEP Network Evaluation.

Although the analysis performed by the TPEP or TPEP Network Evaluation provides valuable information for the security of a system, it does not replace the need for system approval and accreditation. Every environment is unique and must be analyzed for the overall security of the system and the data to be processed by the system. The accreditation process provides an avenue for this unique evaluation to be conducted.

## E. CERTIFICATION AND ACCREDITATION

Certification and accreditation are the terms used to describe the process of analyzing a computer system to determine the level of security afforded based upon a defined security policy and a set of security features. Specifically, certification refers to the technical evaluation of a system and accreditation is the formal declaration that a system is approved to operate in a specific security mode for a specified period of time.

Accreditation assigns responsibility for the operation of the system to the Designated Approving Authority (DAA). Some types of systems may actually require more than one DAA, depending on the environment and the amount of interface with other systems. For example, a system that is connected to a backbone network or a system that supports multiple organizations will require more than one DAA.

Prior to allowing any computer system to process or store classified or sensitive information, the DAA must complete the certification and accreditation process for the system to operate in one of three security modes:

- Dedicated Mode: All users have the appropriate clearance and need-to-know for all of the data processed by the computer system.
- System High: All users have the proper security clearance, but may not have a need-to-know for all of the data processed by the computer system.
- Multilevel Mode: Permits two or more classification levels of data to be processed simultaneously within the computer system. Not all of the users have the appropriate clearance



or access approval for all of the data maintained by the system.

NCSC standard 003-85, *Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* [Ref. 12], provides the government's policy for computer systems which handle classified, sensitive, and unclassified information, as well as details regarding the selection of the appropriate level of trust for any environment. The level of trust is determined by computing the system's risk index which is defined as "the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system." [Ref. 12: p. 5] The risk index is then used in conjunction with a table to determine the appropriate level of trust for the system's environment.

The certification process is the set of procedures used to determine if a system meets the specific security requirements for the operational environment. If all requirements are met, the system will then be accredited by the DAA as meeting the required level of trust. The certification and accreditation process is needed to ensure system users and administrators are able to "trust the system's ability to accurately, consistently, and positively identify each user, and to maintain that positive identification throughout the user's login session. Otherwise, controlled access protection could not be assured, and any audit information collected would be rendered useless." [Ref. 7: p. 22] Specific details regarding who should conduct the certification, the steps

involved in the process, and risk management are provided in the following sections.

### **1. System Analysts**

NCSC recommends the actual system analysis be performed by a team of individuals to ensure the required levels of controlled access protection are provided. All members of the team should have the equivalent of at least a bachelor's degree in Computer Science or Computer Engineering. In addition, at least one member should have expertise in the hardware architectures and all members should have a strong knowledge of the operating systems and a thorough understanding of computer security issues. Prior to analyzing the system, the team should be fully educated on the system's mission, environment, security policy, and any identified threats. [Ref. 7: p. 41]

### **2. Technical Analysis**

The certification and accreditation of a system is performed through a series of interdependent steps. NCSC's *Introduction to Certification and Accreditation* [Ref. 13] manual provides a detailed description of these steps which are briefly described below.

- **Step 1. Assess System Requirements/Assess Tailoring Factors:** The focus of this step is to identify and assess the aspects of the system which are relevant to security. This includes functional requirements, security policies, threat information, mission requirements, security boundaries, and other pertinent data.
- **Step 2. Plan for Certification & Accreditation:** System milestones and resource requirements such as personnel training and equipment purchases should be identified.

Information to conduct the actual system analysis is incorporated into system documentation.

- **Step 3. Perform System Analysis:** The system security attributes as a whole are analyzed. Security measures are assessed and tested with system vulnerabilities and risks identified.
- **Step 4. Report Findings/Recommendations:** The results and recommendations of the previous phases are documented and a certification/accreditation package is developed. The package provides the DAA with a recommendation for an accreditation decision, a statement of residual risk and supporting documentation.
- **Step 5. Conduct Site Survey:** An optional step, a site survey is conducted by the DAA or his/her representative to ensure the security countermeasures meet the system requirements.
- **Step 6. Make Accreditation Decision:** The DAA makes the accreditation decision using one of the following options: full accreditation for the originally intended environment, partial accreditation for operation outside the originally intended environment, interim accreditation approval, or accreditation disapproval. If multiple DAAs are involved, a Memorandum of Agreement (MOA) must be developed and signed as part of the accreditation decision.
- **Step 7. Maintain Accreditation:** Accreditation must be maintained throughout the system's life cycle by ensuring operation continues within the stated parameters of accreditation. Current DOD policy requires a system to be reaccredited every three years, regardless of any changes that may or may not have occurred.

Figure 2 provides a graphical depiction of the overall certification and accreditation process. In addition to these steps, the actual system analysis (step 3) may be further broken down into a separate set of steps. *Assessing Controlled Access Protection* [Ref. 7] describes each of these steps in detail and provides a graphical depiction of the entire process.

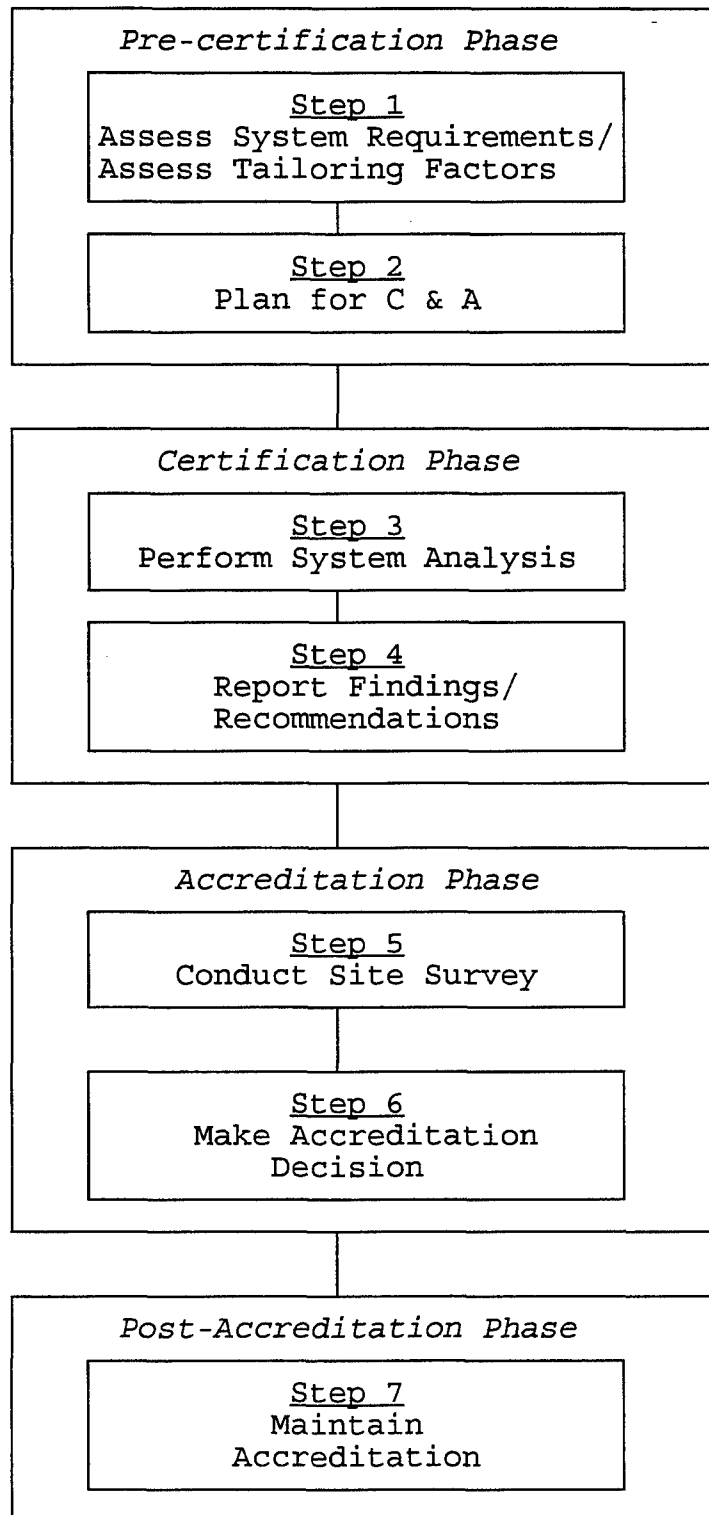


Figure 2. Certification and Accreditation Process  
[Ref. 13: p. 8]

### 3. Risk Management

"Because absolute security is neither technically nor theoretically attainable in a multi-user system, determining whether a system is 'secure' is essentially an exercise in identifying risks and counterbalancing those risks against protection mechanisms. Therefore, the ultimate objective of any security program is risk management." [Ref. 7: p. 53] Risk management encompasses the total process of identifying, measuring, and minimizing uncertain events which can affect the computer system.

Risk management begins with a risk analysis of the computer system which evaluates the relative costs and benefits of security measures and identifies those measures which are acceptable to reduce the level of risks to the system. The term risk is used to identify a measure of the potential loss to a computer system from a threat and the system's vulnerability to that threat. Risk analysis is an on-going process which occurs throughout a system's life cycle. As such, it is a tool used by the DAA to ensure the system's security policy is being enforced at an appropriate level relative to the assumed risks. Once a system is accredited, the need for risk analysis/management does not end, rather it begins.

There are numerous checklists available which may be used to assist with risk management. For example, the book Computer Security: A Comprehensive Controls Checklist [Ref. 14] provides a very thorough checklist for assessing the threats to a computer system. The checklist was designed for an Air Force installation

and "provides a number of controls for each major type of threat against an information system." [Ref. 14: p. 11] The controls are presented in list form with provisions for three possible answers: yes, no, and not applicable. For a control to be applicable, the threat must exist and an asset must need protection. If the control is applicable, then a "yes" or "no" is checked to represent that the control does or does not exist within the system. The book also describes how to assign weights to the various requirements so priorities may be assigned. The areas addressed by the various checklists include: personnel policies, system development, training/awareness, organization structure, physical access, data and program access, input/output, processing operations, database and system software, telecommunications, and video display terminal human factors.



#### IV. THE TRUSTED NETWORK INTERPRETATION

Many of the mechanisms defined by the TCSEC are applicable to networked environments as well. However, the TCSEC provides no guidance for its application to networks. In addition, the TCSEC is void in two major areas where networks are concerned. First, while the TCSEC addresses single-system security, networks typically involve many systems with different architectures and different security vulnerabilities. In today's environment of piecemeal systems being interconnected to form a network, an evaluation criterion which helps to ensure a secure network without requiring every component of the network to be fully trusted is needed. By providing explicit design criterion for networks, system designers will be forced to think about the placement of trust within the overall network. Second, the TCSEC primarily addresses the computer security goals of secrecy and integrity by focusing on access to information written on a computer system. Two additional goals, availability and authenticity, are extremely important in networked environments. Because of these voids and due to concerns regarding the transmission of government data over communication networks, a standard format to be used with the evaluation of computer networks was needed.

Building upon the criterion set forth in the TCSEC, the NCSC published the *Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria* [Ref. 15] or "Red Book" in 1987. The TNI is part of the Rainbow Series and was developed to provide further guidance for networks and network components. The



criterion of the TNI may be used to cover the range of networks from isolated local area networks to wide area internetworks.

The TNI is divided into two major sections. Part I breaks down each of the divisions and classes described in the TCSEC and provides an interpretation of the requirements for a networked environment. The same divisions and classes of trust are used (i.e., D, C1, C2, B1, etc.). Since networks require additional security services (e.g., availability, communications security), Part II of the TNI describes specific services which may or may not be required in a network and furnishes a method for assessing those services. The security services included are communications security, denial of service, transmission security, and supportive services (e.g., encryption tools and network management).

Part II of the TNI also describes how the different components of a network may be categorized according to the type of mechanism provided. The four categories are Mandatory Access Control (MAC), Discretionary Access Control (DAC), Audit, and Identification and Authentication. The TNI abbreviates these categories as M, D, A, and I, respectively. A network component may be functionally used for any combination of these categories. Therefore, a total of 16 component types (including no features provided) may be used in a network. Each component is rated according to the corresponding TCSEC functional requirements for that category. The C2+ rating is used to denote that a component meets the Class B3 DAC and audit functional requirements, but does not provide any MAC features. Through this rating structure, components may be combined to

provide an aggregate level of trust. For example, a "D" component which is rated as C2+ may be combined with other components which are given a Class B3 or A1 rating to produce a Class B3 or A1 system. [Ref. 16] (This would only work if the "D" component were given a Class C2+ rating. A Class C2 component could not be combined in this manner.)

The TNI assigns a minimum and maximum rating for each component type. Table 2 provides a listing of the possible component types and the corresponding rating range.

| Component Type | Minimum Class | Maximum Class |
|----------------|---------------|---------------|
| M              | B1            | A1            |
| D              | C1            | C2+           |
| I              | C1            | C2            |
| A              | C2            | C2+           |
| DI             | C1            | C2+           |
| DA             | C2            | C2+           |
| IA             | C2            | C2+           |
| IAD            | C2            | C2+           |
| MD             | B1            | A1            |
| MA             | B1            | A1            |
| MI             | B1            | A1            |
| MDA            | B1            | A1            |
| MDI            | B1            | A1            |
| MIA            | B1            | A1            |
| MIAD           | B1            | A1            |

Table 2. Component Types and Corresponding Rating Classes  
[Ref. 15: p. 196]

#### A. PART II SECURITY SERVICES

The security services described in Part II of the TNI are rated according to their functionality, strength of mechanism, and level of assurance. Functionality refers to the objective the security service is to fulfill and the approach used to meet that objective. The features provided by the service and its

performance are included under the heading of functionality. The strength of the mechanism measures how effectively the service meets its objective. Both direct and indirect threats to the network must be considered in determining the strength of the mechanism. Finally, assurance refers to the level of trust the users may place on the service that it will achieve the desired functionality. Tamper resistance, verifiability, and the inability to bypass the service are three aspects which must be considered in rating the level of assurance.

Evaluation of the services provided in a network is qualitative and results in a rating of none, minimum, fair, or good. In some cases, the functionality of a service may be described as either none or present, if rating the degree of functionality may not be appropriate. The term none is normally used to describe if the service does not support the strength of the mechanism criterion. Finally, if a security service is not offered, then the term not present is used as the rating. Table 3 was taken from the *Trusted Networks Interpretation Environments Guideline* [Ref. 17] and provides a breakdown of the security services and the range of ratings that may be used for each criterion.

The security services addressed are not required by every network. Similarly, the strength of the service required will vary from network to network according to the operational environment in which it is used. Selecting the appropriate security services for a network is a management decision. The *Trusted Networks*

*Interpretation Environments Guideline* [Ref. 17] provides a series of questions the manager may use to determine the services that are needed and the functionality required. Once it has been determined that a service is required and the functionality has been identified, the strength of the mechanism and the level of assurance is determined through a risk index which is also provided in the TNI guideline.

| Network Security Service                       | Criterion                              | Evaluation Range                                  |
|--|--|---|
| Communications Integrity/<br>Authentication    | Functionality<br>Strength<br>Assurance | None, Present<br>None - Good<br>None - Good       |
| Communications Field<br>Integrity              | Functionality<br>Strength<br>Assurance | None - Good<br>None - Good<br>None - Good         |
| Non-Repudiation                                | Functionality<br>Strength<br>Assurance | None, Present<br>None - Good<br>None - Good       |
| Denial of Service/<br>Continuity of Operations | Functionality<br>Strength<br>Assurance | None - Good<br>None - Good<br>None - Good         |
| Protocol Based Protection                      | Functionality<br>Strength<br>Assurance | None - Good<br>None - Good<br>None - Good         |
| Network Management                             | Functionality<br>Strength<br>Assurance | None, Present<br>None - Good<br>None - Good       |
| Compromise Protection/<br>Data Confidentiality | Functionality<br>Strength<br>Assurance | None, Present<br>Sensitivity Level<br>None - Good |
| Traffic Flow<br>Confidentiality                | Functionality<br>Strength<br>Assurance | None, Present<br>Sensitivity Level<br>None - Good |
| Selective Routing                              | Functionality<br>Strength<br>Assurance | None, Present<br>None - Good<br>None - Good       |

Table 3. Evaluation Structure for Network Security Services  
[Ref. 17: p. 27]

## B. ENSURING TRUST

Any network evaluated using the TNI must have a rational Network Security Architecture and Design (NSAD) which addresses the security relevant policies, objectives, and protocols. The interfaces and services which are needed for the network to be evaluated as a trusted system must be specified as well as the security functionality of the various components.

Just like a stand-alone system, the network also maintains a Trusted Computing Base (TCB) which is referred to as the Network TCB (NTCB). The NTCB includes all of the security-relevant components of the network. In contrast to the "stand-alone system, the design and evaluation of the network rests on an understanding of how the security mechanisms are distributed and allocated to various components, in such a way that the security policy is supported reliably in spite of (1) the vulnerability of the communication paths and (2) the concurrent, asynchronous operation of the network components." [Ref. 15: p. xvii] When a NTCB is distributed over several network components, the portion of the NTCB within a given component is referred to as an NTCB partition.

For a network to be evaluated at a specific class, the network as a whole must meet every requirement for that class as outlined in Part I of the TNI. This does not mean that every network component must satisfy all of the requirements. For example, one component may rely on another component to meet a specific requirement. Neither component will satisfy the requirement individually, but together the requirement is met for the network.

### **C. CERTIFICATION AND ACCREDITATION**

Products are submitted to the NCSC for evaluation in a network environment using the TNI criterion the same way stand-alone systems are evaluated using the TCSEC. However, since there are additional security concerns with a network environment, additional testing is required. Although a product completes the formal evaluation process conducted by the NCSC and may be certified to run at a specific level (e.g., Class C2), the NCSC evaluation process does not eliminate the need for system certification and accreditation. As described in the previous chapter, a network must be evaluated and accredited for operation in its specific environment the same as a stand-alone computer. However, if the network uses a commercial product that has been evaluated and certified by the NCSC, reports from that process may be used as input to the systems certification.

There are two distinct views which may be used to certify and accredit a network. It may be viewed as a collection of two or more interconnected separately accredited computer systems, or it may be accredited as one large system. The view which is selected will have a major impact on the security features required and the level of assurance of the system. Therefore, the desired approach must be defined prior to the start of the certification process.

#### **1. Interconnected Accredited System View**

This view recognizes that parts of a network may be independently created, managed, and accredited. The interconnected

system consists of multiple systems which may be viewed as devices or components to which the other systems may transfer information. Each individual system or "device" must be assigned a sensitivity level for the information it processes.

When evaluating an interconnected accredited system, two additional security problems must be considered: propagation of local risk and the cascade problem. Propagation of local risk refers to the security of one system being endangered by a weakness in another system which is connected to it. Since the overall system may have several accreditors, one must remember that a risk which is acceptable to one person may not be acceptable to another. Special constraints such as one-way connections, cryptographic isolation, or other measures may be imposed on a system to help limit the amount of risk introduced to the overall system.

The cascade problem exists when subsystems are connected in a manner which results in the overall system covering a larger sensitivity range than the individual systems are accredited to handle. In this case, an attacker may be able to exploit the network connections in order to leak information across the range of sensitivity levels. This depends on the cooperation by malicious software between the various subsystems. Several approaches may be taken to prevent this problem from occurring.

- Configuration controls may prohibit the introduction of new software or software which has not been appropriately examined.
- Increasing the trust requirements for the various subsystems may increase the protection mechanisms to a level that is appropriate for the potential compromise.

- Some network connections may need to be eliminated from the overall system.

Both the TNI and the *Trusted Network Interpretation Environments Guideline* discuss the propagation of local risk and the cascade problem in greater detail. In addition, information is provided on how the problems may be identified if they exist in a network and how they may be solved.

Finally, adopting the Interconnected Accredited System view may result in a very complex system which cannot be practically evaluated using the TNI criterion. In that case, the system "accreditor is forced to accept the risk of assessing the security of the network without the benefit of an evaluation against the principles of the TCSEC." [Ref. 15: p. xiii]

## **2. Single Trusted System View**

This view treats the overall network as a single trusted system which is accredited by one authority. "The single trusted system implements a reference monitor to enforce the accesses of subjects to objects in accordance with an explicit and well defined network security policy." [Ref. 15: p. xiv] In addition, the NTCB is partitioned among the various network components which interact through the communication channels. The NTCB partitions must be implemented so the network security policy is enforced for the network as a whole. This approach is normally not as complex as the interconnected system approach and may result in a more secure level of trust in a system.





## **V. THE FALCON LAN - APPLYING THE TCSEC/TNI CRITERION**

The Naval Security Group Detachment (NSGD) Monterey is the Naval contingent of the Defense Language Institute (DLI). As such, NSGD is responsible for the training and well being of the Navy students at DLI. During the fall of 1995, NSGD installed the Falcon Local Area Network (LAN) to assist with their charter to provide administrative, educational, and communication support for both students and staff personnel. The majority of the hardware and software purchased for the LAN was provided by NSGD's headquarters, Commander Naval Security Group (CNSG), and the backbone installation was performed by NISE WEST.

### **A. SYSTEM FUNCTIONALITY AND GOALS**

The NSGD staff has defined the following functional requirements for the Falcon LAN. Since the initial installation of the LAN, not all of the requirements have been met. Those which have not been met are scheduled for future implementation.

- *Provide a Communications System:* The LAN provided a backbone communication system for the various NSGD offices located in two different buildings. Specifically, the LAN joined the Learning Center and administration offices in building 629 with the Commander's office and yeoman offices in building 616 using a client-server structure.
- *Provide a Student Tracking System:* The LAN included the development of a unified database for tracking student information including student course assignment and completion, barracks room assignments, security clearance information, past performance information and other information relating to the individual student.

- *Provide for Service Management:* Access was needed to the DLI student database, Navy Integrated Training Requirements and Resources System (NITRAS), and the Army Training Requirements and Resources System (ATRRS) programs to allow for the assignment of students to language curriculums to meet service needs and student eligibility requirements.
- *Provide for Supply and Fiscal Tracking:* Access was also required to the Naval Postgraduate School supply system, the new supply and purchasing system, and on-line catalogs and supply status servers.
- *Provide Career Counseling Assistance:* A provision for the maintenance and access to the student database with career counseling information such as Armed Services Vocational Aptitude Battery (ASVAB) scores, next duty assignment, and prospective gains and losses was also needed. In addition, the LAN was to provide the Educational Services Officer with course completion, Personnel Advancement Requirements (PARS) and other advancement information and provide personnel with access to the Bureau of Naval Personnel (BUPERS) bulletin board and detailee electronic mail.
- *Provide for Command Information Dissemination:* The LAN was to provide a route for the dissemination and tracking of command welcome aboard packages, provide NSGD personnel with access to the World Wide Web (WWW) server, and provide outside access to the Defense Language Institute NSGD home page.
- *Allow for the sharing of electronic mail with DLI:* Access to and compatibility with the DLI Microsoft Mail server was needed to allow the transfer of electronic mail between the staffs. In conjunction with this, all NSGD Staff and Navy and Marine students needed electronic mail accounts to allow for the free exchange of electronic mail within the command and with other DLI electronic mail users.
- *Provide for the Instruction of the Cryptologic Technician Apprentice Common Core Curriculum using the LAN:* To complete the automation of all NSGD requirements and provide total connectivity, connections with the Educational LAN in the Learning Center were needed. This would allow for interactive CD-ROM instruction of the Cryptologic Technician Apprentice Common Core Curriculum and provide a CD-ROM library for access by the LAN.

In addition to the functional requirements specified above, one additional function was desired for the LAN - to provide the ability to receive unclassified message traffic using the Defense

Message System (DMS). Currently, all message traffic (classified and unclassified) is received on a stand-alone personal computer running an awkward program called Above Board. Unclassified message traffic is screened and then distributed on the LAN using a CNSG-approved program called Message Board. The actual progress made to date in achieving these requirements will be discussed further in the section on interoperability.

Command goals for the Falcon LAN include: system expansion into every barracks room, limited access by all students for educational use, electronic mail use, and remote login to educational services like the Cryptologic Technician Apprentice Common Core Curriculum. Additionally, the LAN should be configured to easily accept future software and hardware expansion and upgrades. (Note: The software and hardware expansion/upgrades will require the system to be re-accredited.)

## **B. SYSTEM CONFIGURATION**

### **1. Users**

The total number of personnel supported by the Falcon LAN is approximately 375. This includes access by 35 staff personnel and approximately 340 students. The mix of students is normally 40 officers and 300 enlisted personnel. Proposed future expansion of the LAN will also permit access by approximately 100 Marines stationed at DLI.

Access to the LAN for the majority of staff personnel is required between 0630 and 1700 weekdays. The supply officer is the

exception to these hours, requiring access through 2000. Specific processing requirements for each of the staff offices are:

- **Database Manager and Professional Development:** Requires the ability to access the network for database management and to input information into the NSGD student database.
- **Quota Manager:** Requires the ability to access and update the NSGD student database and the DLI student database, to access the CNET's NITRAS and the Army ATRRS programs, and to access the BUPERS bulletin board and electronic mail services.
- **Division Officer and Information Security Manager:** Requires LAN access for database management and access to the NSGD student database.
- **Supply Officer:** The supply officer is responsible for ordering over 400 supply items, administering a \$100,000 per year budget and maintaining all controlled equipment. Unique requirements for this office include the ability to access the supply HICK (hazardous material list), FedLog (stock number access), Naval Logistics Library, and Perform Pro (Government forms).
- **Command Career Counselor and Educational Services Officer:** Requires the ability to input information into the NSGD student database.
- **Yeoman:** The Yeomen are divided into two sections that handle student administration and command functions. They require the ability to input information into the NSGD student database.

In addition to the internal access requirements, several of the staff offices also require outside access to various agencies. Specifically, outside E-mail and File Transfer Protocol (FTP) access is required for the offices as follows:

- **Database Manager and Professional Development:** Access to the Chief of Naval Education and Training (CNET) and the Commander Naval Security Group (CNSG) is required.
- **Quota Manager:** Outside access is required with DLI, CNET, Army NITRAS, and BUPERS.

- **Division Officer and Information Security Manager:** Requires outside access with DLI, CNET, and CNSG.
- **Supply Officer:** Outside access is required with DLI logistics, DLI Information Management, the Naval Postgraduate School (NPS), CNSG, Navy Comptroller, and commercial vendors.
- **Command Career Counselor and Educational Services Officer:** Outside access is required with CNET, CNSG, and BUPERS.
- **Yeoman:** Require access to CNET, CNSG, BUPERS Access, DLI, and NPS.

## 2. Hardware

### a. Computers

Thirty Intel 486DX2-66 MHz Energy Star Systems provide access to the LAN for the various LAN users. These systems include 14-inch Video Graphics Array (VGA) monitors, 16 MBytes of Random Access Memory (RAM), 340 MByte hard drives, and Etherlink III network cards.

### b. Servers

The LAN servers include one Pollywell Pentium 100 MHz Redundant Arrays of Inexpensive Drives (RAID) System set to RAID level 5 with mirroring, 12 GBytes of hard drive space, 65 MBytes of RAM, a CD-ROM, and a tape backup. Two additional servers are Pentium 100 MHz machines with 32 MBytes of RAM, 1.2 GB hard drives, CD-ROM, and a tape backup. The 1.2 GB hard drives are MAXTOR MXT-SCSI 1240S models with fast Small Computer System Interface-II (SCSI-II) connections. The tape backup units are WANGTEX model 51000ES with a capacity of 1.0 GBytes and they are SCSI compatible.

The CD-ROM units are Phillips Sony CM 225MS models and are multi-session capable.

**c.    *Printers***

Three Epson Action Laser 1000 printers with 2 MBytes of memory each provide printing capability to LAN users. The printers can be upgraded to a maximum of 6.5 MBytes of memory each using 256 KByte chips. The majority of the workstations in the staff offices have a local printer attached and available for use by all LAN users.

**d.    *Internal Cabling***

The Falcon LAN is an Ethernet 10Base2 network using Thin Net RG-223 coaxial cabling and BNC connectors to provide internal connectivity. Links within building 629A join the Learning Center computers used by Navy students with office computers used by the Navy staff. Building 616, the Navy's Administration building, uses Thin Net cabling to connect a series of computers used by the Commanding Officer (CO), Executive Officer (XO), and additional Navy staff.

**e.    *External Cabling***

The Presidio of Monterey (POM) Facility Area Network (FAN) provides the campus backbone for DLI and is managed by the Directorate of Information Management (DOIM). Major features of the FAN include an IBM 3174 mainframe computer, a 48-strand multi-mode fiber optic backbone, and a CISCO AGS+ router to which

six token ring 802.5 LANs are attached. The token ring upon which the mainframe is resident provides a 56 Kbps telephone link to the NIPRNET, the replacement for the Defense Data Network. The FAN was used to provide the external connectivity between buildings 629A and 616 as well as connectivity to the "outside world" through the CISCO router.

DLI's fiber optic plant consists of a 48-strand multi-mode backbone from building 343, the location of the Cisco AGS+ router, to building 617, with connections to 92 buildings on campus, including buildings 616 and 629A. An optical transceiver completes the connection between buildings 616 and 629, and the AGS+ Cisco router by performing the required ethernet-to-optical conversions and vice versa.

### **3. Software**

Within Building 629A, 30 PCs provide processing capability for an estimated 400 students. Physically located in the student Learning Center, these computers have WordPerfect 6.0 and language software applications. Additional applications, learning programs and electronic mail may be added to the network in the future.

Windows NT 3.51 is the Network Operating System (NOS) used on the servers. In addition to Windows NT, the client workstations use the Windows 95 operating system with the following applications available to staff personnel: WordPerfect 6.0, MS Office Professional with Bookshelf, Lotus 123, and Harvard Graphics. The Structured Query Language (SQL) server provides access to SQL, Paradox, NITRAS, ATRRS, and Harvard Graphics.



### C. CLASS C2 REQUIREMENT

The National Security Agency (NSA) has stipulated that all computer systems operated by cryptologic organizations must achieve the following minimum level of trust by calendar year 2000: [Ref. 18]

| <u>Operational Mode</u> | <u>Class of Trust</u> |
|-------------------------|-----------------------|
| Dedicated               | C2                    |
| System High             | C2                    |
| Compartmented           | B1                    |
| Multilevel              | B2                    |

According to the *Information System and Network Security Procedures for Service Cryptologic Elements* [Ref. 18], the Falcon LAN is categorized as a cryptologic Automated Information System (AIS) since it directly supports the efforts of the cryptologists assigned to DLI. Although the information stored on the Falcon LAN will be unclassified, due to the sensitivity of Privacy Act information it should be considered as operating in the System High mode. This classification would be used since all system users will have the appropriate clearance (in this case unclassified), but some will not have a valid "need-to-know" for some of the data contained in the system. Therefore, the Falcon LAN would be required to meet the Class C2 requirements by calendar year 2000.

### D. WINDOWS NT VERSION 3.51 OVERVIEW

Windows NT Workstation and Windows NT Server are 32-bit, graphical oriented operating systems which support popular Windows-

based applications, preemptive multitasking, and symmetric processing. [Ref. 19] "Windows NT Workstation is optimized to provide a high level of interactive application responsiveness, while Windows NT Server provides optimized network responsiveness." [Ref. 20: p. 4] Specific workstation features which were optimized (when compared to earlier versions of the software and other network operating systems) include overall reduction of memory usage, higher system priorities for interactive applications, and improved efficiency of both 16-bit and 32-bit applications. Similarly, the server features which were optimized include improved memory usage (by caching large amounts of data), higher system priorities for network users, and improved efficiency for 32-bit server operations. Normally the name Windows NT is used to reference both products.

Both Windows NT Server and Windows NT Workstation were tested by the NCSC for Class C2 compliance with the requirements set forth in the TCSEC. The hardware platforms used in the evaluation included two different processor architectures: Intel Pentium microprocessor (Compaq Proliant 2000 and 4000 (Pentium)) and the DEC Alpha AXP/150 with the DECchip 2106-AA processor. It is important to note that the testing performed was for a stand-alone configuration only. Therefore, Class C2 compliance in a networked environment using Windows NT has not been granted. The *Final Evaluation Report* [Ref. 21] of 14 February 1996, was written by the NCSC evaluation team and provides a comprehensive summary of the

results for the overall evaluation. It was the primary reference used throughout this section.

Before evaluating Windows NT and the Falcon LAN against the TCSEC, an overview of the Windows NT software is needed. The following sections are provided to create a foundation for the evaluation that is conducted in Section E of this chapter.

### **1. The Trusted Computing Base (TCB)**

Three components make up the Windows NT Trusted Computing Base (TCB): [Ref. 21: p. 5]

- *Executive*: runs the processor privileged state or kernel mode.
- *Protected Servers*: run the processor unprivileged state, called user-mode.
- *Administrator Tools*: run in user mode.

Figure 3 provides a graphical representation of the overall TCB. Due to space limitations, not every executive subsystem or individual protected server has been drawn. However, the I/O Subsystem and Memory Manager have been identified to show the interaction with the hardware. In addition, it should be noted that the device drivers, microkernel, memory manager, and Hardware Abstraction Layer are all hardware dependent.

#### **a. The Executive**

The executive is further divided into three conceptual layers which are referred to as the Hardware Abstraction Layer (HAL), the Microkernel, and the "rest" of the executive or executive subsystems.

The HAL "provides an abstract view of the underlying machine architecture to the executive, allowing for a machine-independent implementation of Windows NT executive (thereby allowing Windows NT to be easily ported within machines of similar architectures." [Ref. 21: p. 5] The information provided to the executive by the HAL includes machine-specific details regarding functions such as device Input/Output (I/O), processor initialization, and interrupts.

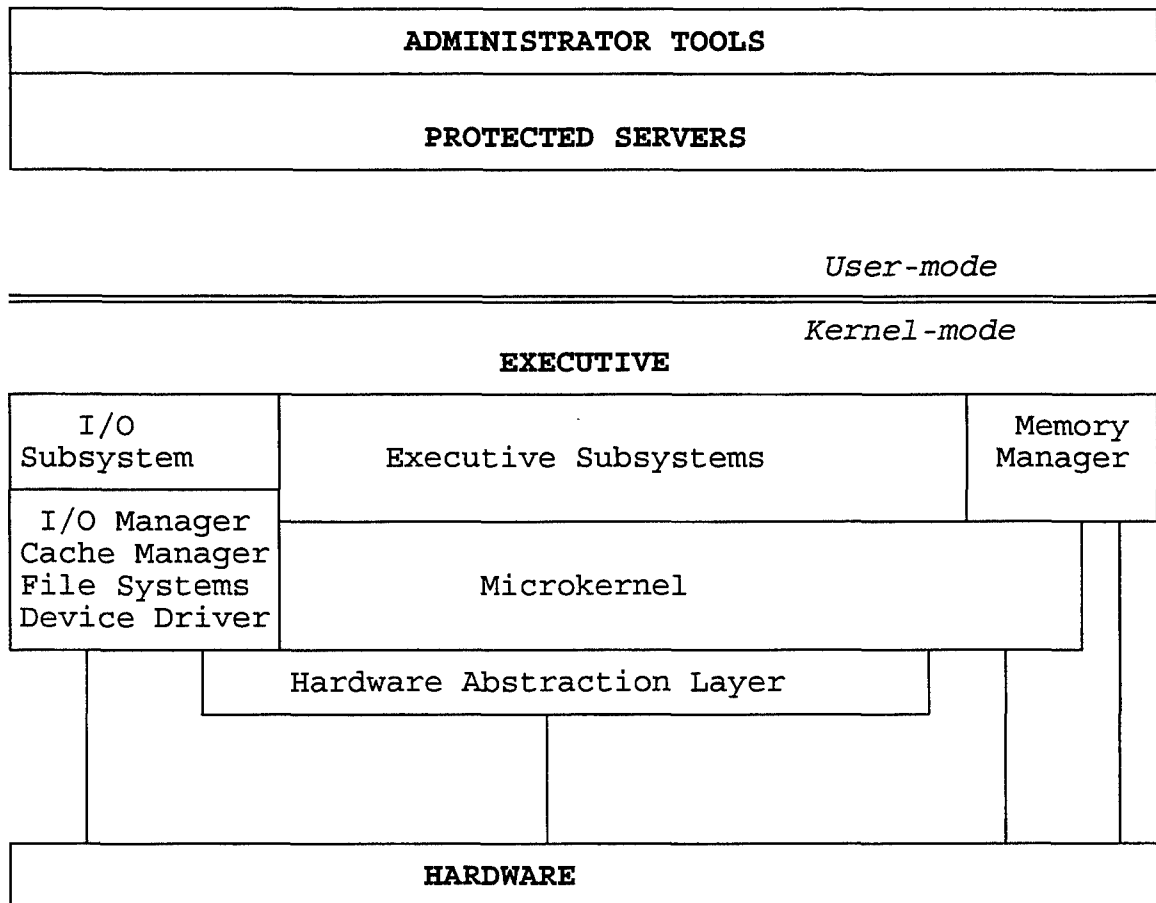


Figure 3. Windows NT Operating System Overview [Ref. 21: p. 6]

The Microkernel provides the foundation for the rest of the executive subsystems, giving low-level support for execution, interrupt and exception handling, and synchronization. Some of the primitive objects created by the Microkernel are exported to user-mode programs from the executive by the Executive Object Services and Process Manager.

The executive subsystems include the following:

- **Object Manager:** The Object Manager is responsible for the creation, access, and deletion of objects used within the executive and exported from the executive. The Object Manager is also responsible for managing handles and handle tables. Every process has a handle table which identifies the objects currently accessed by it. For a process to gain access to an executive object, the process must first acquire a handle (a ticket that permits access) from the Object Manager. The Object Manager works with the Security Reference Monitor to validate if the process is authorized access, generates the handle (if permitted), and then adds the handle to the object's handle table. The handle identifies the type of access allowed (i.e., read, write, execute) and limits the type of access to only those permitted. The Object Manager manages three types of objects: type, directory, and symbolic link. The "type" object is used only within the executive. It provides the executive subsystems with the ability "to create classes of objects (e.g., directories, files, processes, semaphores) and define their semantics." [Ref. 21: p. 7]
- **Security Reference Monitor:** This subsystem generates the checks for access control and privilege validation and is also responsible for audit generation. The Security Reference Monitor exports security services to user-mode processes through the generation of tokens which are used by the protected servers to validate access requests, check authorized privileges, and generate audits for the user-mode.
- **Process Manager:** "Windows NT executive provides multi-threaded processes. Essentially, a process is a private virtual address space, associated physical memory, and a set of accessible objects. A thread is a point of execution within a process, and includes all necessary execution

context information (e.g., registers, stack pointers). A process may have zero or more threads." [Ref. 21: p. 7] A process with no threads cannot execute. The Process Manager exports both processes and threads as executive objects.

- **Virtual Memory Manager:** This subsystem provides a demand-paged memory management system for the executive. Every process has a private page table directory which identifies the location of various page tables. The page tables in turn identify the location of pages of memory. Combined, the page table directories and page tables are used to identify memory locations. Page-level memory protection features are included for read, write, and execute access. Sections of shared memory between processes are exported by the Virtual Memory Manager as an executive object type.
- **Local Procedure Call (LPC) Facility:** Communication between processes is supported through the LPC Facility. It may export executive object ports for communication support outside of the executive.
- **Input/Output (I/O) Subsystem:** The I/O subsystem includes the I/O Manager, the file systems, and the various device drivers; and provides packet-driven, asynchronous I/O. Some device drivers may have a layered structure, with each layer depending upon the services of the lower layers. The I/O Manager facilitates the communication between the layers. The Cache Manager is used by the file system to support memory-mapped I/O and provide a memory-based cache.
- **Configuration Manager:** The Configuration Manager maintains the system configuration information through a registry. The registry is implemented in a tree-structured database that is indexed by keys. Keys are the executive type object which may be exported by the Configuration Manager.
- **Executive Object Services:** The Executive Object Services along with the Process Manager provide interfaces between the user-mode and exported executive objects.

#### ***b. Protected Servers***

Protected Servers are user-mode processes which provide security relevant services. The Protected Servers which were included in the Windows NT software evaluated by NCSC included: the Local Security Authority (LSA) subsystem, WinLogon, Win32, the

Security Accounts Manager (SAM), the Print Spooler, the Session Manager, the Service Controller, and the Event Logger. [Ref. 21: p. 8] The following provides a brief description of each protected server:

- **Local Security Authority (LSA):** Maintains the list of valid user identifiers and their associated passwords. It is also used to collect and store audit records.
- **WinLogon:** Coordinates user authentication upon login by prompting the user for an identifier and password. The information is validated by the LSA before system access is permitted.
- **Win32:** Provides the interface to Windows NT through two user-mode exported objects, WindowStation and DeskTop. The WindowStation object provides the means for a user to access and manipulate the various system resources, such as the keyboard, mouse, and display. The DeskTop object provides the user with abstract resources such as menus, windows, and title bars. Every DeskTop object must have an associated WindowStation object. Both types of objects are protected and audited through the use of services provided by the Security Reference Monitor.
- **Security Accounts Manager (SAM):** Provides security administration of user accounts.
- **Print Spooler:** Routes print requests to the appropriate printer.
- **Session Manager:** Initiates the WinLogon and Win32 protected servers during system initialization and starts other system processes as needed. The Session Manager works with the WinLogon and Service Controller to authenticate user access and identify security attributes.
- **Service Controller:** Manages drivers and services by monitoring the current status of each. Also ensures the loading of all drivers which require automatic loading at boot-time.
- **Event Logger:** Writes audit records into a log file and provides services for processes to enter events into the log. Services are also provided for the log entries to be viewed by authorized personnel.

**c. Administrator Tools**

|                    |  |
|--------------------|--|
| Backup             | Provides functions to back up disk files to tape, restore tape files to disk, label, track, and identify tapes.  |
| Chkdsk             | Checks for and identifies file integrity problems; also examines security descriptor information of NTFS partitions.   |
| Control Panel      | Permits users to customize and administer Windows NT; security relevant features include the administration of the computer clock, device drivers, ports, print manager, Registry services, and system performance parameters. |
| Disk Administrator | Provides functions to partition disks, create and delete volume sets, extend volume sets, create and delete stripe sets, establish and break mirror sets, and recover data.  |
| Event Viewer       | Allows for viewing, sorting, filtering, and searching event logs.  |
| File Manager       | Provides file and directory manipulation and organization functions.   |
| Print Manager      | Provides functions to manage printing, printers, and print jobs.   |
| Program Manager    | Basic user interface used to organize the applications and files in groups and to start the applications easily.   |
| Registry Editor    | Used to view and edit the configuration database.  |
| Setup              | Used to accomplish the original installation of Windows NT; allows administrators to make several configuration changes.   |
| User Manager       | Used to create and manage user accounts and groups, and to implement the security policy.  |

Table 4. Administrator Tools [Ref. 21: pp. 128 - 131]

The Administrator Tools provide resources for managing all aspects of the Windows NT System. Included are tools for managing user accounts, auditing the system configuration, performing file system backups, and reviewing audit records. The specific set of



tools which were included in the NCSC evaluation were: "Backup, Chkdsk, Control Panel, Disk Administrator, Event Viewer, File Manager, Print Manager, Program Manager, Registry Editor, Setup, and User Manager." [Ref. 21: p. 9] Table 4 provides a brief description of each of these tools.

#### **d. TCB Interfaces**

There are three methods through which an untrusted subject may request services from the TCB:

- **Unprivileged Hardware Instructions:** The untrusted subject may invoke any unprivileged hardware instruction (e.g., arithmetic operations).
- **Windows NT Executive System Services:** The untrusted subject may make a call to the executive system services.
- **Interprocess Communication (IPC):** The untrusted subject may make a request of one of the protected servers.

A large set of Dynamic Link Libraries (DLLs) provide the programming interface to the Windows NT system. When a function is initiated by one of the DLLs, it will result in at least one of the above service requests.

## **2. Subjects**

In Windows NT, a subject is a process with one or more threads. Each process has an associated virtual address space, a private handle table, and a security context. Every thread within the process has equal access to the address space and private handle table. Security context information is provided by access tokens which contain access control and privilege information.

Every process has exactly one primary token which represents the current user and his or her authorized access permissions.

Windows NT also permits a technique referred to as impersonation in which one process may adopt the security attributes of another process. For example, this may occur when a server process impersonates a client process in order to obtain access to objects maintained on the client. Each thread within a process may have one impersonation token which is used to accomplish this task.

### **3. Objects**

Two broad categories of objects are used by Windows NT: executive objects and server objects. The executive objects are created, managed, and protected by the various executive subsystems and the server objects are created and maintained by the user-mode protected servers. The Object Manager and Security Reference Monitor provide access mediation for all executive objects. In contrast, server objects are protected by the corresponding TCB protected server which may request services from the Security Reference Monitor in the executive. Table 5 provides a breakdown of the various types of objects and the corresponding subsystem which is responsible for the object's security and management.

| <b>Executive Object Types</b>                          |                                |
|--|--------------------------------|
| <i>Object Type</i>                                     | <i>Managing Subsystem</i>      |
| Event  | Executive Object Services      |
| Event Pair   | Executive Object Services      |
| I/O Completion Port                                    | Executive Object Services      |
| Key  | Configuration Manager          |
| Mutex  | Executive Object Services      |
| Object Directory                                       | Object Manager                 |
| Object Symbolic Links                                  | Object Manager                 |
| Port   | Local Procedure Call Facility  |
| Process  | Process Manager                |
| Profile  | Executive Object Services      |
| Section  | Memory Manager                 |
| Semaphore  | Executive Object Services      |
| Thread   | Process Manager                |
| Timer  | Executive Object Services      |
| Tokens   | Security Reference Monitor     |
| Device   | I/O Manager and Device Drivers |
| Mailslot   | Mailslot File System           |
| Named Pipe   | Named Pipe File System         |
| NTFS File  | Windows NT File System         |
| NTFS Directory   | Windows NT File System         |
| <b>Protected Server Object Types (user accessible)</b> |                                |
| <i>Object Type</i>                                     | <i>Managing Server</i>         |
| Log  | Event Logger                   |
| Service  | Service Controller             |
| Desktop  | Win32 Server                   |
| Print Job  | Print Spooler                  |
| Printer  | Print Spooler                  |
| Print Server   | Print Spooler                  |
| WindowStation  | Win32 Server                   |

Table 5. Windows NT Protected Objects [Ref. 21: p. 141]

Every object may have one or more of the following attributes associated with it:

- **Owner ID:** Identifies the owner of the object. The owner may be an individual, a global group, or a local group. The owner always has the WriteDAC and ReadControl permissions for the object. WriteDAC allows the DACL to be modified and

ReadControl allows an object's security information to be read.

- **Discretionary Access Control List (DACL):** The DACL provides the primary means for controlling access to an object. The DACL entry identifies the permissions granted or explicitly denied to a user or group of users.
- **System Access Control List (SACL):** A system administrative structure, the SACL is used to control security auditing for the object.
- **Group ID:** Used to provide compatibility with certain operating system standards, such as POSIX. It has no security relevance.

Container and non-container are two additional terms which are used to define objects within Windows NT. Specifically, a container object is one which logically contains other objects. For example, a directory would be defined as a container object since it contains files. In turn, the files are examples of non-container objects since they do not contain other objects. [Ref. 22]

#### 4. Object Access Rights

An access mask is the DACL entry used to denote the types of access permitted or denied to an object. A standard structure is used for all types of objects to ensure the "Security Reference Monitor (SRM) can perform access validation regardless of the specific object type." [Ref. 21: p. 142] Although the access mask structure is standard, the meaning of some fields within the mask may be type specific and are defined by the executive subsystem or protected server responsible for managing the object.

Five types of access rights may be specified by an access mask: standard, specific, generic, Maximum Allowed (MA), and Access system Security (AS). MA and AS rights are used only with requests for access to an object. Specifically, MA is used to request all permitted access rights to the object and AS is used to request access to the object's SACL.

The standard access rights are interpreted the same for all objects, regardless of type, and include five permissions: [Ref. 21: p. 143]

- **Delete:** Permits an object to be deleted.
- **ReadControl:** Permits an object's security related information (e.g., owner, DACL) to be read.
- **WriteDAC:** Permits modification of the DACL.
- **WriteOwner:** Permits a thread to change the ownership of an object to any security identifier within the thread's current token.
- **Synchronize:** Permits the object to be used for process synchronization.

The synchronize permission is normally used only for specific types of objects such as communication or process objects. The other four permissions are used for all types of objects.

Specific access rights are completely type-specific and have no general meaning. The access mask may contain up to 16 permissions which are defined by the responsible executive subsystem or protected server.

Finally, generic access rights are not actually access rights to an object, but rather a reference to standard and/or specific

rights. The reference is a mapping to a subset of the other rights. There are four generic access rights: GenericRead, GenericWrite, GenericExecute, and GenericAll. GenericAll is structured to map to all of the standard and specific rights of the specified object type.

## 5. Privileges

"Privileges are stored in a process' token and allow a thread to take exception to an object's DACL or utilize restricted services." [Ref. 21: p. 151] The privileges of a process are determined by the privileges assigned to the account of the user who has invoked the process. A privilege may be used by a thread at any time. The subsystem which implements and audits the privilege is referred to as the enforcer. Examples of privileges are:

- **CreateToken:** Creates a token; enforced by the SRM.
- **AssignPrimaryToken:** Assigns the primary token of a process; enforced by the Process Manager.
- **Security:** Identifies the holder as a security operator, permitting access to SACLs and the audit log; enforced by Win32, Object Manager, SRM, NTFS, Event Logger.
- **LockMemory:** Locks physical pages in memory; enforced by the Memory Manager.
- **Backup:** Needed to perform backup operations; enforced by the Configuration Manager, I/O subsystem, and NTFS.
- **SystemTime:** Permits the system time to be changed; enforced by the Executive Object Services.

## **6. File System Types**

Windows NT supports five distinct types of file systems including the File Allocation Table (FAT) system, the Windows NT File System (NTFS), the CD-ROM File System (CDFS), the Named Pipe File System (NPFS), and the Mailslot File System. NTFS is a new file system which was specifically designed for Windows NT. It is not supported on floppy diskettes and only NTFS files are protected by Discretionary Access Control (DAC).

Any environment with security concerns should use the NTFS file system because it provides more security features than the standard FAT system. If a FAT system is used, the Secure System Partition command from the Disk Administrator utility may be used to partition the FAT in its entirety.

## **7. C2Config.EXE**

To assist with establishing a Class C2 compliant system, an application called C2Config was created and included in the Windows NT Resource Kit [Ref. 23]. The program allows the user to select and implement the appropriate settings for Class C2 security. A graphical display with a lock next to each security aspect indicates which requirements have been satisfied (locked) and which requirements have not been met (unlocked). In addition to the indication of being locked or open, a color scheme is used to denote which requirements are mandatory for Class C2 compliance. Specifically, a red lock indicates an explicit requirement and a blue lock represents an optional feature. The various attributes

and their descriptions as defined on screen by the Windows NT Resource Kit are: [Ref. 23]

- **File Systems (Required):** Under Windows NT, only the NT File System (NTFS) supports DAC to the files and directories. Consequently, only NTFS volumes are allowed on the system to provide secure and auditable access to the files. FAT volumes do not provide the necessary security functions to support Class C2 level security.
- **OS Configuration (Required):** Allowing other operating systems, such as MS-DOS to run on a secure system, can allow users to circumvent Windows NT security. For a system to support Class C2 level security, Windows NT must be the only operating system on the computer.
- **OS/2 Subsystem (Required):** The OS/2 subsystem was not included in the current NCSC Class C2 evaluated configuration. For a system to conform to the evaluated configuration, the OS/2 system must be disabled. The C2Configuration manager disables the OS/2 subsystem by deleting the following files from the SYSTEM32 directory under the systemroot: OS2.EXE and OS2SS.EXE.
- **POSIX Subsystem (Required):** The POSIX subsystem was not included in the current NCSC Class C2 evaluated configuration. For a system to conform to the evaluated configuration, the POSIX system must be disabled. The C2Configuration manager disables the POSIX subsystem by deleting the following files from the SYSTEM32 directory under the systemroot: PSXSS.EXE.
- **Security Log (Required):** Class C2 level security requires that a security audit log be maintained and the events in the log may not be automatically overwritten. For systems that do not require Class C2 level security, other logging options may be selected such as to overwrite events that are older than a certain age or when the log is full.
- **Halt on Audit Failure (Optional):** If the security log is full, it becomes possible for some events to not be logged. Selecting this option will halt the computer when the log is full to prevent losing any events. If the system halts as a result of a full log, an administrator must restart the system and reset the log.
- **Display Logon Message (Optional):** On a secured system, a warning message may be displayed before the user is allowed to log on. Typically this message will inform the user that the system is authorized for users only and that



unauthorized use is considered trespass or is unwelcomed. In contrast, if the system is used in a public forum, the message may be used to inform the user of current events or how to log onto the system.

- **Last Username Display (Optional):** Displaying the name of the last user can make logging in more convenient, however, hiding the name of the last user can prevent usernames from being accidentally discovered and subsequently used to break into the system. This option allows the username to be hidden when the logon screen is displayed.
- **Shutdown Button (Optional):** Hiding the shutdown button from the logon screen prevents users from shutting the system down without first logging onto the computer. This option should only be selected if the power switch and reset button is not accessible by the user. Even though the shutdown button may be hidden, if the user has access to either the reset button or the power switch, they may still turn the system off without properly shutting down the operating system.
- **Password Length (Required):** The longer the password, the less likely it will be discovered randomly, or deliberately by an intruder. Class C2 level security does not allow Blank Passwords. Using this item, the desired password policy can be selected.
- **Guest Account (Required):** The Guest account allows anonymous and therefore unauditible access to the system and its files. Class C2 level security does not allow for anonymous access to the system and therefore requires the Guest account to be disabled or deleted from the system. When this item is selected, the Class C2 Configuration manager disables all Guest accounts.
- **Networking (Required):** Not currently cleared for networks.
- **Drive Letters and Printers (Optional):** To prevent redirection of data to a device or port that may not be authorized, the assignment of drive letters and printer ports can be restricted to administrators only.
- **Removable Media Drives (Optional):** Since Windows NT is a multi-user system, programs run by other users may be running in the background while a user is logged on. It is possible to prevent programs run by other users from accessing disks in removable media drives that may have been inserted while a user is logged on by allocating these drives automatically when a user logs on.

## **E. EVALUATING THE LEVEL OF TRUST**

Since the computer system implemented at DLI is a network, the TCSEC criterion as interpreted in the TNI must be used to determine if the system meets the Class C2 requirements. The following sections provide a breakdown of these criterion with an evaluation of the Falcon network. Since the Network Operating System (NOS) is the primary controller of access to the various objects (including applications) on the network, the focus of this evaluation is on Windows NT version 3.51.

### **1. Security Policy**

The first requirement of the TCSEC specifically states that a system must have an "explicit and well-defined security policy enforced by the system." [Ref. 5: p. 3] This means that with the set of all identified subjects and objects within the system, there must exist a set of rules which are used by the system to determine whether or not a subject should be permitted access to an object. At the Class C2 level of trust, this policy will be discretionary and will be enforced using the Discretionary Access Control (DAC) and Object Reuse requirements, at a minimum. The information will be protected to the granularity of individual access rights. In addition, the policy implementation will describe network features which prevent or detect the unauthorized reading or destruction of sensitive information.

It should be noted that the TNI does not include operators, system programmers, technical control officers, and system security

officers under the title of users. These positions are considered support personnel and are subject to the requirements of the Trusted Facility Manual and the System Architecture. [Ref. 15: p. 16]

The network security policy may require data secrecy, data integrity, or both. The secrecy policy defines the DAC mechanisms used to prevent the unauthorized reading of sensitive information, and the data integrity policy defines the mechanisms used to prevent the unauthorized modification (i.e., writing) of sensitive information. Due to the amount of sharing in a networked environment, the integrity of the data stored is just as important as the secrecy of the data. Therefore, most networks will address both data secrecy and data integrity in the overall security policy.

**a. Discretionary Access Control (DAC)**

*Requirement:* The DAC portion of the security policy must define and control the access of objects by subjects within the system to the individual user level. Groups of individuals may also be given control rights, provided the individual members of the groups are identified by the group name. This includes network identifiers such as internet addresses for various components of the network. In addition, the DAC mechanism must limit the propagation of access rights with only authorized subjects being permitted to grant access rights to unauthorized users of an object.

*Windows NT Features:* Windows NT uses Discretionary Access Control Lists (DACLS) to regulate access between subjects and objects with access controlled to the granularity of an individual user. The entries are used only with the NTFS file system. Each entry represents access granted or explicitly denied to a user or group of users. The DACL also permits users to share objects with other users or groups of users. The owner of an object or any user with WriteDAC access to the object, may define access restrictions on the object. NT does not require every object to have a DACL associated with it. If an object does not have a DACL, then any user who is able to name and open the object is permitted all access rights. This is not the same, however, as an empty DACL which means no one has access to the object.

The DAC policy is enforced by the Security Reference Monitor (SRM). When access to an object is requested by a subject, the SRM compares the subject's token to the object's DACL. If the subject is requesting access to an executive object, the request must be made through the Object Manager which in turn performs the validation with the SRM. Once it has been determined that access is permitted, a handle is created and access is granted (see section D.1.a, Object Manager description). After a handle has been stored for a subject in the executive object's handle table, all subsequent access requests are verified by using the access mask that is stored as part of the handle.

If the subject is requesting access to a protected server object, the object must be opened before access is permitted. Once

the request is made by the subject, the protected server sends a validation request to the SRM to verify that access is authorized. If access is permitted, the SRM exports a handle with the appropriate information and the object is opened (i.e., access is granted). Unlike the executive objects, this process must be accomplished for all subsequent requests by the subject as well.

There are six privileges which may override the rights listed in the DACL. If any of these privileges are enabled on the primary or impersonation token of the subject requesting access, the DACL is overridden. The exception privileges include TakeOwnership, Security, Backup, Restore, Debug, and ChangeNotify.

When an object is created, the DACL may be directly assigned, assigned by default, or inherited. If directly assigned, the parameters which define the DACL are passed by the object create system call. The default assignment is used for objects which are required to have a DACL. This includes all named executive objects, server objects, process, thread, and token objects. When the object is created, the values assigned to the DACL are based upon the user creating the object, any explicit values provided in the create process, default values from the creating process token, and any inheritable DACL information. Finally, sub-objects of container objects may inherit DACL information from the container or parent object. Control flags which are part of the DACL entry may be used to limit the amount of inheritance permitted.

### **b. Object Reuse**

*Requirement:* Object reuse pertains specifically to the storage objects within a computer system and is used to ensure the secrecy of information once a portion of memory or storage space has been reallocated. Specifically, the TNI states:

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. [Ref. 15: p. 20]

As applied to a networked environment, the object reuse criterion requires the NTCB to ensure a storage object does not contain information for which the subject is not authorized access before granting the subject access rights. This requirement must be enforced by every portion of the network that contains storage objects.

*Windows NT Features:* "All resources, including executive and non-executive objects, visible at the TCB interface are appropriately handled with respect to object reuse." [Ref. 21: p. 180] The object reuse requirements are fulfilled by the executive or non-executive subsystem which is responsible for creating and maintaining the object. Reuse protection is provided in three ways: [Ref. 21: p. 153]

- All fields in the object's header and body are initialized to new values as appropriate.

- The memory allocated for an object is written over with zeros.
- Only the data that has been written most recently may be read and nothing more.

For objects such as files which may require frequent changes, access controls in addition to the DACL are provided by the use of high water marks and end-of-file markers. The high water mark indicates the largest size of the file prior to current access. When a new process accesses the file, the subject may enlarge the file, moving the end-of-file marker. When this occurs, the file system immediately zeros the space on the disk or tape between the old high water mark and the new end-of-file marker, thus prohibiting any process from reading beyond the previous end-of-file marker. [Ref. 21] The same process is used for any object which requires frequent backups to disk in order to minimize the amount of dynamic memory required.

Hardware reuse is controlled by the executive subsystems, WinLogon, or Win32 and includes the use of integer and floating point registers, VGA memory, and special purpose registers. The reuse requirements are met by clearing all storage locations when one interactive user logs out of the system or upon reallocation of the storage. Specifically:

- Processor registers are initialized to a known state when a thread is started. When the context changes, the processor state is saved and all registers (except floating point) are reinitialized. Floating point registers are saved and reinitialized when a floating point instruction is issued by a new context.

- VGA memory is cleared and can no longer be displayed when an interactive user logs off.
- I/O hardware (e.g., drive controller status registers, keyboard buffers, and data caches) require administrative or system privileges to access. Any attempt to access these objects by an unauthorized subject will result in a general exception and access is denied.
- Printer buffers are cleared by printer language code which is sent to the printer prior to each print job.

## **2. Accountability**

### **a. Identification and Authentication**

*Requirement:* All users must identify themselves to the TCB before it can be expected to mediate any actions on their behalf. A protected mechanism such as a password must be used to authenticate the user's identity, and all authentication data must be protected from unauthorized disclosure. The TCB must be able to enforce accountability with the granularity of an individual user through unique identification of all users and auditing of user actions.

In a networked environment, the identification and authentication may be performed by either the individual component to which the user is connected or some other component. Authentication information may be passed between components of the network (NTCB partitions) without reauthentication, provided the data is protected from unauthorized disclosure or modification. Most networked environments use a network interface card (e.g., Ethernet card) in the computer systems for authentication.

*Windows NT Features:* To logon to the system, Windows NT requires every user to be identified with a unique username. The



username is represented internally by a Security Identifier (SID) which cannot be reassigned to another user. When the user initiates a process, his or her SID is incorporated in the process' primary token and is used for auditing of all security related events.

Windows NT permits passwords to be used in conjunction with the username. The passwords are encrypted and stored in the Security Accounts Manager (SAM). When a user logs onto the system, the Local Security Authority (LSA) checks with the SAM to ensure the username and password provided are authentic before granting the user access to the system.

There are some serious concerns with respect to identification and authentication in a networked Windows NT environment. First, the Windows NT configuration evaluated by the NCSC did not use a secure network interface card to ensure authentication. Second, a remote utility permits administrators to manage all network users from anywhere on the network provided the appropriate trust relationships have been established between users and groups of users. Should the administrator's logon identification and password be compromised, the remote utility could be used by a "masquerader" with full access to the network through the remote utility. In general, Windows NT server does not provide any protection against intruders beyond the password.

## **b. Audit**

*Requirement:* An audit trail of access to objects protected by the TCB must be provided. The specific auditing requirements outlined in the TCSEC are:

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity. [Ref. 15: p. 22]

In the networked environment, the auditing capabilities may be provided by one or more components with data transmitted to a designated collection point. Auditing capabilities are to be provided for both local and remote access; and provisions must be made to protect the data from loss due to resource inavailability.

*Windows NT Features:* The Local Security Authority (LSA), Security Reference Monitor (SRM), protected servers and executive subsystems, Event Logger, and Event Viewer combine to provide the auditing mechanism for Windows NT. The LSA defines which events are to be audited and passes the appropriate parameters (i.e.,

auditing enabled flag and event categories) to the SRM. "The event categories are: detailed tracking, system, logon/logoff, object access, privilege use, policy changes, and account management." [Ref. 21: p. 159] The event types included in each event category are listed in Table 6 along with the subsystem which is responsible for generating the audit record.

Audit records for the detailed tracking, system, object access, and privilege categories are constructed by the SRM. In order for an audit record to be generated, the responsible subsystem or protected server must send a request to the SRM that an audit record be made for each occurrence of the specified event. Any executive subsystem can initiate such a request, but user-mode protected servers must have the Audit privilege before making the request. The Audit privilege is identified in the primary token of the process initiating the request.

The actual audit records are written to a log file by the Event Logger. In turn, the system administrator may read the security log or generate a report by using the Event Viewer. A user must have either the Security privilege or be granted access to the security log through its DACL in order to use the Event Viewer to view the file. Read and write permission provided by the DACL is limited to members of the Administrative group only, and

| Category             | Event Type                                      | Constructor |
|----------------------|---|-------------|
| System               | System Restart                                  | SRM         |
|                      | System Shutdown                                 | SRM         |
|                      | Authentication Package Loaded                   | LSA         |
|                      | Registered Logon Process                        | LSA         |
|                      | AuditLog Cleared                                | SRM         |
|                      | #Audits Discarded (due to full internal queues) | SRM         |
| Logon/<br>Logoff     | Logon Successful                                | LSA         |
|                      | Unknown User or Password                        | LSA         |
|                      | Time Restricted Logon Failure                   | LSA         |
|                      | Account Disabled                                | LSA         |
|                      | Account Expired                                 | LSA         |
|                      | Invalid Workstation                             | LSA         |
|                      | Logon Type Restricted                           | LSA         |
|                      | Password Expired                                | LSA         |
|                      | Failed Logon                                    | LSA         |
|                      | Logoff  | LSA         |
| Object<br>Access     | Open Object                                     | SRM         |
|                      | Close Handle                                    | SRM         |
| Privilege<br>Use     | Assign Special Privilege                        | SRM         |
|                      | Privileged Service                              | SRM         |
|                      | Privileged Object Access                        | SRM         |
| Detailed<br>Tracking | Process Created                                 | SRM         |
|                      | Process Exit                                    | SRM         |
|                      | Duplicate Handle                                | SRM         |
|                      | Indirect Reference                              | SRM         |
| Policy<br>Changes    | Privilege Assigned                              | LSA         |
|                      | Privilege Removed                               | LSA         |
|                      | Audit Policy Change                             | LSA         |

| Category           | Event Type                  | Constructor |
|--------------------|-----------------------------|-------------|
| Account Management | Domain Changed              | LSA         |
|                    | User Changed                | LSA         |
|                    | User Created                | LSA         |
|                    | User Deleted                | LSA         |
|                    | Global Group Member Removed | LSA         |
|                    | Global Group Member Added   | LSA         |
|                    | Local Group Changed         | LSA         |
|                    | Local Group Created         | LSA         |
|                    | Local Group Member Removed  | LSA         |
|                    | Local Group Member Added    | LSA         |
|                    | Local Group Deleted         | LSA         |

Table 6. Audit Event Types [Ref. 21: p. 160]

the Security privilege is only assigned to administrators. Each audit record contains the following information:

- Time event was generated
- SID of the process generating the event
- Name of component or module submitting the event
- Event ID
- Type of event: error, warning, success, information, success audit, failure audit.
- Event category
- Computer

Figure 4 details the flow and interaction of the auditing scheme provided by Windows NT.

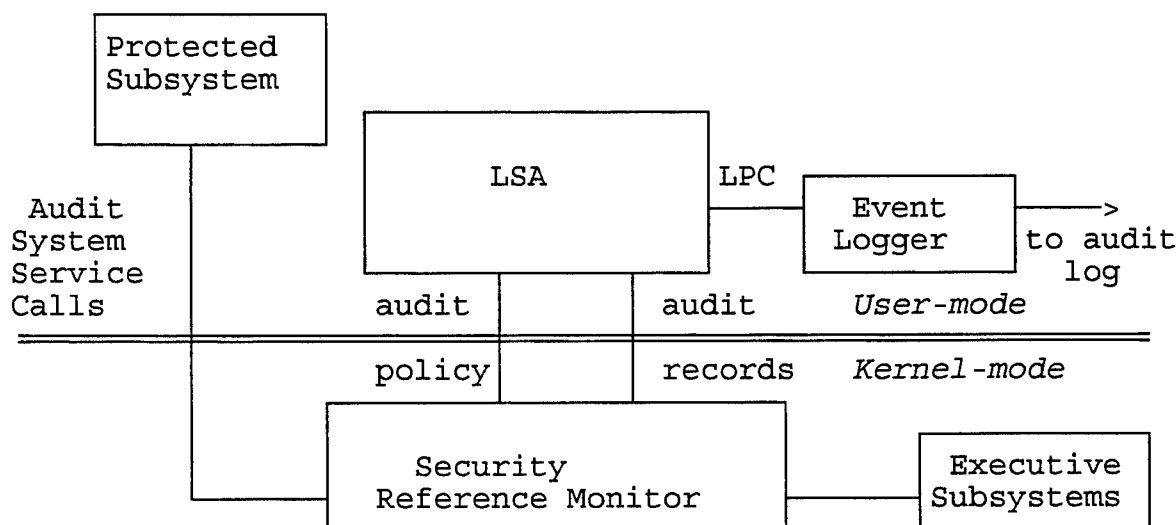


Figure 4. Windows NT Audit Flow [Ref. 21: p. 158]

There are three situations which may cause audit records to be lost:

- The SRM internal queues reach their high water mark.
- The security log file becomes full.
- The LSA internal queues become full.

The system can be configured to prevent a loss of records in these instances. Specifically, the wrap around option for the security log should not be selected, and the security log should be the maximum size available with a registry key flagging the system to halt when the file becomes full. These options are set by the administrator using the Event Viewer.

Despite the security features of Window NT, there is one vulnerability which can permit the features to be bypassed. This was demonstrated in the spring of 1995 and reported in Government Computer News in September. Specifically, the article by Paul Constance sites:

According to DOD security criterion, a Class C2 rating is supposed to guarantee that an operating system can prevent unauthorized access to specific files on a computer and generate an unerasable audit trail of attempts to gain access. But at the Armed Forces Communications and Electronic Association's TechNet conference in Washington this spring, dozens of attendees watched as Robert Wainright, a Camden, N.J., computer security consultant, used commercial utilities to read, copy and delete protected data on the hard drive of a PC running Microsoft Windows NT - all without leaving a trace.

Wainright exploited the so-called "boot floppy" vulnerability of PCs with Intel Corp. microprocessors and floppy disk drives. By interrupting a normal boot-up from the hard drive, a user can invoke the system setup routines and boot from the floppy. Using assembly language utilities, an intruder then can read, copy or delete files from the hard drive, all without invoking the OS and its security features. [Ref. 24]

The reason this vulnerability was not a factor in the evaluation conducted by the NCSC was due to the "fact that the two Proliant computers from Compaq Computer Corporation on which Windows NT was evaluated had floppy drives that were disabled." [Ref. 24] Typically, NSA will refer vulnerabilities such as this to the area of "physical security" which includes measures such as removing the floppy drive every night or installing a Fortezza encryption card to increase the difficulty for an intruder attempting to boot from the floppy. Ultimately, the responsibility for ensuring this

vulnerability is not taken advantage of lies with the system administrator who oversees the level of access granted to system users. In a networked environment, the importance of this vulnerability is drastically intensified with the network points of access distributed throughout buildings and across campus and should not be ignored.

### **3. Assurance**

#### **a. Operational Assurance**

*Requirement:* The System Architecture shall be designed to protect the TCB from external interference or tampering. Protected resources (e.g., subjects and objects) shall be isolated in a manner which enforces access control and auditing requirements. In a networked environment which partitions the NTCB, each partition will provide protection over the resources within its domain.

System integrity is achieved through hardware and software features which may be periodically used to ensure the correct operation of the hardware and firmware elements of the TCB. Features must also be available for validating the correct operation of a new component before it is added to the network configuration. If a failure is detected, it must be reported to the network administrator for further investigation.

*Windows NT Features:* Several execution domains within the TCB are used to provide protection from external interference and tampering. The executive is protected by running in the hardware kernel-mode (i.e., privileged mode), and the protected servers and Administrator tools are all executed through a TCB process. The



TCB processes are "protected through the address space isolation mechanisms of the executive." [Ref. 21: p. 183] Finally, on-disk storage and data structures are protected through the use of the DACL mechanism. Through these features and the audit and control mechanisms, Windows NT protects all system resources.

For the system integrity requirements, Microsoft has several packages which may be requested for system testing and hardware validation on various platforms. For example, a processor diagnostic kit is available for Pentium processors as well as hardware compatibility test suite for the system and peripherals. In addition, most computer manufacturers can provide a suite of diagnostic tests which demonstrate that the hardware is performing properly. These diagnostics should be run prior to loading Windows NT on the computer and revised periodically throughout the life of the system to ensure the hardware is performing correctly.

#### ***b. Life-Cycle Assurance***

*Requirement:* Security testing must be performed to ensure the security mechanisms act in the manner described in the system documentation. In particular, testing should focus on the potential for an unauthorized user to bypass or defeat a security mechanism and search for flaws which would permit unauthorized access to audit or authentication data.

*Windows NT Features:* The testing performed by Microsoft on Windows NT treated each component as a separate "black box" and focused on three distinct aspects: [Ref. 21]

- Testing the security-relevant functionality of the protected servers, the executive, and the various Application Programming Interfaces (APIs).
- Testing major security-relevant mechanisms including object access protection, object reuse, and the use of privileges.
- Testing all security-relevant access to the TCB from the administrative tools user interface.

Both automatic and manual tests were conducted on both Windows NT Server and NT Workstation. "In general, the security-relevant APIs of the protected servers and the executive were tested automatically by programs that exercised numerous calls to the APIs, each with different arguments or different test configurations." [Ref. 21: p. 169]

#### **4. Documentation**

##### **a. Security Features User's Guide**

*Requirement:* The manufacturer must provide user documentation which describes the protection mechanisms provided by the TCB, interprets their use, and describes how the subsystems or components interact with one another.

*Windows NT Features:* The *Windows NT Security Features Users Guide (SFUG)* provides the following information:

- Description of the Windows NT TCB and its protection mechanisms.
- "How to" information concerning logging onto Windows NT, changing user's passwords, locking and unlocking the computer, and using a screen saver.
- Explains how to place a DACL on a file or directory and describes what ownership means.

**b. Trusted Facility Manual**

*Requirement:* This manual is addressed to the system administrator and identifies functions and privileges which should be controlled. Information concerning the review and maintenance of audit files in particular, is addressed. In addition, procedures for assisting with configuration management (including physical and administrative controls) must be provided.

*Windows NT Features:* The *Windows NT Trusted Facility Manual* fulfills these requirements by describing "privileged built-in groups whose membership should be controlled" and identifying the privileges and special abilities they provide. [Ref. 21: p. 185] Auditing capabilities are also described in detail and the record structure for every type of audit event is provided. Finally, the various administrative tools are presented and discussed.

**c. Test Documentation**

*Requirement:* This documents the overall testing process by identifying the test plan, describing procedures for testing security mechanisms, and furnishing the results of functional testing.

*Windows NT Features:* Following the security testing conducted by Microsoft, the appropriate test documentation was created and supplied to the NCSC during the product evaluation. The documentation described the tests conducted, the security mechanisms, and the administrative tools. In addition, an overview document was provided which detailed the purpose and goal of each test suite. Overall, the test documentation supplied to the NCSC

was determined to be sufficient "with respect to both breadth and depth of coverage." [Ref. 21: p. 185]

**d. Design Documentation**

*Requirement:* The design documentation describes the manufacturer's security philosophy and explains how it is translated into the TCB. When the TCB consist of distinct modules, the interfaces between the modules are also described. For a network environment with a partitioned NTCB, the security policy and partitioning of the NTCB are described as well as the allocation of security requirements among components. All relevant components and their method of interconnection must be documented and evaluated in order for the security of the entire network to be validated. The Network Security Architecture and Design is the document which normally details the specifics concerning the interface between components of the network.

*Windows NT Features:* There are numerous documents and texts available covering almost every aspect of Windows NT. Overall, the system is very well documented. Both the Windows NT 3.5 Guidelines for Security, Audit, and Control and the Windows NT Resource Kit provide great detail with respect to security features and mechanisms. However, despite a thorough review by the NCSC of the documentation provided on Windows NT, a review of the Network Security Architecture and Design was not conducted. Therefore, assurance regarding the network design has not been provided by NCSC.

## **5. Additional TCSEC Features**

In addition to the Class C2 level requirements, Windows NT also met two B2 level requirements in the testing conducted by the NCSC. Specifically, the NT platform was evaluated against the B2 Trusted Facility Management and B2 Trusted Path functional requirements.

For the B2 Trusted Facility Management requirement, the TCB must separate operator and administrator functions. This was met by the software's ability to grant an arbitrary subset of rights to a user, enabling the role of "operator" to be defined according to local requirements. "In addition, built-in groups, like Backup Operator and Power Users allow users to perform well-defined roles without providing the full range of capabilities associated with administrator accounts." [Ref. 21: p. 187] This follows the popular principle of "least privilege" which was introduced by Jerome Saltzer and Michael Schroeder in their paper "The Protection of Information in Computer Systems." [Ref. 25]

For the B2 Trusted Path requirement, a trusted communication path between the TCB and the user must be supported for initial logon and authentication, with communication initiated strictly by the user. Windows NT provides a trusted path and uses the Secure Attention Sequence (Ctrl, Alt, Del keys pressed simultaneously) to initiate the logon and authentication process by the user. In turn, this sequence guarantees the communication will be with the WinLogon server and not another process. Therefore, control through the trusted path is provided for the user to logon, logoff,

shutdown the system, lock the workstation, or change their password.

Although Windows NT meets the B2 level requirements for the Trusted Facility Management and Trusted Path, it was not evaluated against any assurance requirements above the Class C2 level. Therefore, the overall evaluation rating remained at Class C2.

## **6. Other Security Services**

Part II of the TNI describes the other security services which are relevant to a networked environment. The following sections provide an individual analysis of the Falcon LAN as compared to each of these services. As discussed in chapter 5, each service is rated according to its functionality, strength of mechanism, and assurance. The ratings assigned to the Falcon LAN for each service are based upon the research conducted in support of this thesis.

The following sections describe the functionality and strength of mechanism requirements for each service and applies these requirements to the Falcon LAN. The assurance provided for each mechanism is concerned with the level of confidence the service provides in meeting any threat to the mechanism. This is determined by ensuring the mechanism has been implemented correctly and the objectives of the service have been achieved. The assurance for every service is evaluated with a rating in the range of none to good.

### **a. Communications Integrity**

Communications integrity refers to several security services which are concerned with the "accuracy, faithfulness, non-

corruptibility, and believability" of information that is transferred between components of a computer or communications network. [Ref. 15: p. 178] The measures used to achieve communications integrity have some strong similarities to the mechanisms used to enforce DAC and MAC requirements. In the networked environment, the communications integrity concerns are defined through three aspects: authentication, communications field integrity, and non-repudiation.

(1) Authentication. The functionality criterion for authentication requires the network to ensure all exchanges of data are established with the addressed component and not with someone attempting to masquerade as another user or replay a previous transmission. Authentication typically follows identification and the system must protect all identification, authentication, and authorization information. Techniques routinely applied to networks to achieve authentication include: passwords, encryption, and mechanisms which use the characteristics and/or possession of the network component or user.

Encipherment or signature mechanisms may be used to provide the authentication service through encryption. With a conventional private-key encryption system, the encryption of a message with a private key automatically implies the authenticity of the data's origin since only the key's holder could have produced the encrypted message. In cases where dishonesty may lead to a dispute over the transmission of an encrypted message, a digital signature scheme may be required for authentication. If a

public-key encryption scheme is used, an encrypted message is authenticated by decrypting it with the public key of the sender, thus providing proof of its origin. The functionality of the authentication service provided in the network is evaluated as none or present, according to the presence or absence of the service.

The strength of the authentication service or mechanism is typically evaluated in the range of none to good. If the service provided is through the use of passwords, the strength of the mechanism is dependent upon the manner in which passwords are selected and protected. Parameters such as the length of the password, its composition, the lifetime permitted, and the protection afforded to passwords must be considered. For a password mechanism to receive an evaluation of good, it must conform to the *Department of Defense Password Management Guidance* [Ref. 26], of 12 April 1985.

If the authentication service is provided through encryption, the mechanism may be combined with handshaking protocols or non-repudiation services (e.g., notarization scheme) to strengthen the service. The overall strength of the service is determined by evaluating the strength of the ciphers, the correctness of protocol logic, and the implementation.

The Falcon LAN uses passwords and the Windows NT TCB to identify and authenticate a user prior to granting access to the system. With Windows NT, a unique Security Identifier (SID) is used to identify every authorized user. The SID is actually several concatenated numerical values which are hierarchical in



nature and of variable length. The SAM stores the username, corresponding SID, and encrypted password in a Registry which is protected by a DACL. The actual authentication procedure with respect to password management was described in the NCSC Final Evaluation Report as follows:

Of particular interest is the storage of account passwords. The User Manager uses a one-way function to hash the password and then temporarily encrypts the hashed password, using a trivial session key, for transmission to the SAM. When the SAM receives the password, it decrypts it, again using the trivial session key, and re-encrypts it using a private key for storage in the user's account in the security accounts database. The private key that the SAM uses is based on the account's user SID.

The main role of the SAM during the authentication process is to provide requested information to the LSA and the authentication package. Again, of particular interest is the user's password. When the password is requested from the SAM, the SAM first decrypts the password, using its private key, and returns the hashed value. Thus, the authentication package is comparing two hashed values, rather than clear text or encrypted values. [Ref. 21: pp. 113 and 115]

Windows NT provides the system administrator with much flexibility for the management of passwords. Specifically, the administrator can invoke the following constraints for each system user:

- Set the minimum password length
- Set an expiration date for the password
- Maintain a history of previously used passwords
- Create a dictionary for screening proposed passwords

The SAM manages these constraints for each user.

The Falcon LAN does not have any other hardware or software features beyond the passwords for authentication purposes. The establishment of a trusted path is critical to authentication in a networked environment. Although Windows NT was evaluated as meeting the Class B2 trusted path functional requirements by the NCSC, the trusted path does not exist external to the individual workstation. Therefore, assurance from the path between nodes cannot be provided. Based upon the password policy enforced, the capabilities provided by Windows NT, and the lack of a trusted path for the overall network, the estimated authentication ratings for the Falcon LAN are provided in Table 7.

| Feature               | Rating  | Comments  |
|-----------------------|---------|---|
| Functionality         | Present |   |
| Strength of Mechanism | Fair    | A trusted path for the overall network would significantly strengthen the authentication services. As for passwords, the only Guidance recommendation not met is that passwords are provided by the system users and not automated. |
| Assurance             | Fair    | Hardware authentication devices such as Fortezza cards would increase the level of assurance provided.  |

Table 7. Authentication Ratings

(2) Communications Field Integrity. Protection from unauthorized modification of any of the fields involved in a communication is referred to as communications field integrity. The header or protocol-information field and the user-data field are the two fields most commonly referred to with respect to data

communications. In addition to these two, other fields may be identified such as control and priority fields.

The mechanism used to ensure communication field integrity counters active threats and protects the data from unauthorized modification. Functionally, the service should ensure the accuracy of the data transmitted from its source to its destination despite possible equipment failure, attempted access by an unauthorized user, or code and format conversions from communication protocols. An automated capability to test for, detect, and report errors should be included as part of the network. In addition, effective countermeasures to address possible attacks to the communications (e.g., jamming, line or node outages, active wiretapping) should be included. These countermeasures may be in the form of security policy and procedures, physical controls, mechanisms, or protocols.

The functionality of the field integrity service is determined through an evaluation of its ability to detect integrity violations. The functionality rating ranges from none to good. Table 8 details the specific requirements for each rating level. For ratings of minimum and fair, either requirement must be provided. Each rating builds on the previous rating and for ratings of fair and good, the requirements of minimum and fair must also be met, respectively.

| Rating  | Required Features  |
|---------|--|
| Minimum | Integrity is provided for a single Protocol-Data-Unit (PDU) (e.g., packet, datagram) through the ability to determine if a received PDU has been modified. |
|         | It can be determined if selected fields within a PDU have been modified.   |
| Fair    | It can be determined if selected fields transferred over a connection have been modified, inserted, deleted, or replayed.                                  |
|         | Any modification, insertion, deletion, or replay of a PDU within a PDU sequence can be detected with no recovery attempted.                                |
| Good    | Any modification, insertion, deletion, or replay of a PDU within a PDU sequence can be detected with recovery attempted.                                   |

Table 8. Basis for Communications Field Integrity  
Functionality Rating [Ref. 15: p. 181]

The strength of the mechanism is determined through the policy, procedures, automated or physical controls, mechanisms, and protocols which ensure the data has not been subjected to excessive random errors and unauthorized modification. Any countermeasures to prevent message stream modifications should be identified and proven to be effective. In addition, the probability of an undetected error should also be identified. An automated capability for testing, detecting, reporting, and/or recovering from communication errors or corruption should be incorporated into the network. The evaluation range used for the strength of the mechanism is from none to good.

The Falcon LAN is an Ethernet 10Base2 network. Therefore, the hardware has the collision detection features of

Ethernet (i.e., if a collision is detected during transmission, a special jam signal is transmitted and the message or packet is resent). Physical controls have also been implemented for the servers and fiber transceivers so only authorized personnel are granted access to the equipment. In addition, use of the TCP/IP protocol provides added checks to the transmission of packets. Beyond these controls, no other security features are currently in place which would relate directly to the communications field integrity service. Although the equipment does test and correct transmission collisions, it does not provide the capabilities described for a minimum functionality rating in Table 9. Therefore, the rating for the communications field integrity would have to be none.

(3) Non-Repudiation. The non-repudiation service "provides unforgeable proof of shipment and/or receipt of data." [Ref. 15: p. 182] This is accomplished by one or both of the following means:

- Providing the recipient of the data with a proof of its origin which will prohibit the sender from denying its transmission or contents.
- Providing the sender with proof a delivery so the recipient cannot deny receiving the transmission or its contents.

Digital signature techniques are the most widely used form of non-repudiation service provided. The technique used may be based on either the signature of the parties or an arbitrated scheme in which a third party validates the signature in

the same manner as a notary public certifies the signatures on paper documents. The functionality of such a scheme is rated as either none or present, signifying the absence or presence of the service on the network.

The strength of the non-repudiation service is determined by the trust given to the underlying cryptography used with the digital signature, the correctness of the protocol logic, and the appropriateness of the implementation. The evaluation range used for describing the mechanism's strength is from none to good. The Falcon LAN does not currently provide any mechanism for this service. Therefore, the functionality rating would be none.

***b. Denial of Service***

Service is denied whenever the throughput on the network falls below a pre-established threshold, access to a remote component is not available, or resources are not available to end users. If a connection is active, the denial of service condition may be detected by monitoring the maximum waiting time or examining the level of throughput on the system. In contrast, when a connection is not currently engaged, there is no way of determining a denial of service attack which cuts off the flow of information unless the network component knows explicitly when data are to be transferred to it. The effects of the denial of service condition should be considered for all network components when determining network service requirements.

(1) Continuity of Operations. Security features aimed at protecting the network against denial of service attacks from external sources may include built-in redundancy throughout the network, distribution of network control functions, fault tolerance mechanisms to prevent hardware failures, and security controls to monitor access and prevent wiretapping. The functionality of the continuity service is evaluated with ratings ranging from none to good. Table 9 identifies the basic requirements for the various ratings.

The strength of the mechanism is also rated from none to good, and is evaluated according to the robustness of the feature and its operational maintenance. Attributes such as error/fault detection, fault treatment, damage assessment, error/failure recovery, component/segment crash recovery, and network crash recovery may be examined during the evaluation process.

| Rating  | Requirement  |
|---------|--|
| Minimum | The service should detect and report conditions which result in a degradation of service below a specified minimum.  |
| Fair    | The service provided for the minimum rating would continue in the event of equipment failure or actions by unauthorized users or processes. This service may be provided from system redundancy, an alternate facility, or some other means. |
| Good    | This is the same requirement as the minimum rating, but with automatic adaptation.   |

Table 9. Functionality Ratings for Continuity of Operations

Continuity of operations features are incorporated on the Falcon LAN through hardware, software, and physical controls. As previously described, the Ethernet backbone has collision detection and recovery features built-in which monitor the transmission of packets. A tape backup system is used to backup crucial data in case a network crash should occur. A full system backup is performed on a weekly basis and incremental backups (which include the registry files) are performed daily. All backup tapes are kept in a vault in a different building than the servers. In addition, an Uninterruptable Power Supply (UPS) provides added assurance in the event of a loss of power.

With Windows NT, the Redundant Array of Inexpensive Drives (RAID) technology has been used to establish a mirror of the server files. RAID is a method of protecting "data by combining smaller, less expensive drives together in a way that data redundancy and security is increased." [Ref. 27: p. 125] The Falcon LAN uses RAID level five which uses parity bits to reconstruct damaged data. A total of 6 GBytes of data are mirrored between two of the servers.

Finally, physical controls imposed on the location of the servers protect them from physical access by unauthorized individuals, and cabling is visually inspected for wiretapping. In addition, LED indication lights on the hub may be used for monitoring access to the LAN.

The majority of these features are aimed at protecting physical assets and restoring information in the event



of a system failure. However, the Falcon LAN is missing mechanisms which would help detect and report conditions resulting in a degradation of service. For example, if someone were to flood the network with packets, there is no mechanism in place to detect the attack. Or, if a node on the network were to experience a degradation in service, there is no mechanism to detect the reduction. Mechanisms such as protocols which ping network nodes for availability would further strengthen the assurance for continuity of operations on the Falcon LAN. Balancing the lack of detection and reporting services with the fault tolerance features provided, the ratings for continuity of operations are estimated to be minimum for all three features: functionality, strength of mechanism, and assurance.

(2) Protocol Based Protection. Denial of service mechanisms are often protocol based and can involve testing or probing the network. In an attempt not to increase network overhead, existing communications availability services should be used whenever feasible. Typically, the rating used for the functionality of this service is based upon the number of protocol based mechanisms provided. Specifically, one mechanism would equate to a rating of minimum, two or three mechanisms are considered fair, and three or more would be rated as good.

The strength of the mechanism is normally determined through off-line testing and/or simulation. "Network protocol robustness may decrease inversely with network loading" and the testing should address this possibility. [Ref. 15: p. 187] In

addition, the evaluation should test for both internal failures and external attacks. Upon completion of all testing, the mechanism is assigned a rating between none and good for strength.

Windows NT supports numerous transmission protocols. As a default, NT uses the Network Basic Input/Output System (NetBIOS) Extended User Interface (NetBEUI) as the actual transport protocol. [Ref. 27: p. 39] NetBEUI operates at the session layer of the Open Systems Interconnection (OSI) reference model and is responsible for synchronizing and sequencing the packets in a network connection, ensuring the connection is maintained until transmission is completed, and ensuring appropriate security measures are taken during the session. [Ref. 28: p. 730]

Windows NT also supports the Transmission Control Protocol/Internet Protocol (TCP/IP), the Data Link Control (DLC) protocol, and the Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocol. DLC is typically used with token ring networks to handle communications between microcomputers and mainframes. The IPX/SPX protocol is the main protocol used by Novell and provides communication between Netware products and Windows NT. Finally, TCP/IP is the main protocol used by NT to support internetworking. [Ref. 27: pp. 39-40] The TCP/IP protocol suite is a "connection- and stream-oriented, transport layer protocol" which uses the IP portion at the network layer to actually deliver the packets. [Ref. 28: p. 809]

The Falcon LAN uses both the NetBEUI and TCP/IP protocols for transmission with Windows NT. However, no testing or

simulation has been conducted with these protocols to fully determine the level of protection provided within the Falcon LAN. Therefore, ratings for protocol based protection must be based upon the wide-spread use and testing of these protocols. Overall, the rating is estimated to be fair for all three: functionality, strength of the service, and assurance.

(3) *Network Management.* Network management focuses on the overall health of the network, detecting failures and reduction in levels of service. Any network management protocols or tools should detect problems in these areas and report them to the system administrator. The functionality of such tools are rated as either none or present.

"Integrity and adequacy of control in a network are the keys in coping with denial of service conditions." [Ref. 15: p. 188] Fault tolerance mechanisms must be in place to deal with both internal failures and external attacks. The strength of the mechanisms provided are evaluated and assigned a rating in the range of none to good.

The Falcon LAN does have several fault tolerance mechanisms in place to guard against internal failures. (These were described previously under the continuity of operations section.) These features which are in place would also be useful in the event of a line being cut or a segment of the LAN being taken out of service. Other than the fault tolerant features and a staff devoted to monitoring the daily operation of the LAN, there are no other tools or features implemented. In addition, as

previously noted, the LAN is lacking mechanisms which would detect and report system failures. Overall, the functionality rating for the LAN would be present and the strength of mechanism and assurance ratings for the overall services provided are estimated to be fair. If other tools such as a firewall and a detection/reporting mechanism were added, the strength and assurance ratings could be higher.

**c. Compromise Protection**

Compromise protection refers to security services which are concerned with the secrecy and non-disclosure of information between components on the network. These features may be provided through administrative, technical, or physical means.

(1) Data Confidentiality. Data confidentiality guards against the unauthorized disclosure of information, normally through passive wiretapping or an unauthorized release of a message. Physical protection and encryption are the most common forms of protection used in networks. The functionality of this service is rated as none or present to indicate the absence or existence of the service within the network.

Through physical protection and encryption, the release of a message and traffic analysis can be prevented. For encryption mechanisms, the NSA normally evaluates the strength of the mechanism for a given environment and provides the sensitivity level of the data the mechanism is approved to protect. In turn, the sensitivity level is used as the evaluation level for this service.

The Falcon LAN does not currently use any encryption packages to protect data that is transmitted. Although physical security measures have been taken to secure the servers and transceivers, each workstation on the network provides a point of access. The LAN does use the Windows NT time-out feature, which requires a password be provided for access if the computer has been sitting idle for a period of time. This reduces the probability that one can gain access to a computer left idle, but does not eliminate the threat. Since the network administrator and his staff cannot possibly be everywhere continuously to ensure personnel are logging off when done with their system and unauthorized users are not attempting to use workstations, the data confidentiality service must be rated as none.

(2) Traffic Flow Confidentiality. This aspect of confidentiality guards against the unauthorized disclosure of information through traffic analysis. "Traffic flow confidentiality is concerned with masking the frequency, length, and origin-destination patterns of communications between protocol entities." [Ref. 15: p. 190] Physical protection, encryption, and traffic padding are the primary mechanisms used to guard against the traffic analysis threat. The functionality of the service is normally rated as none or present, and the strength of the mechanism is evaluated in the same manner as the strength of the data confidentiality mechanism.

Again, the Falcon LAN does not have any mechanisms or features which would provide this service. Therefore, the rating for traffic flow confidentiality is also none.

(3) Selective Routing. The routes over which data travel in a network can be selected through dynamic routing or prearranged paths. In some cases, certain paths or nodes may need to be avoided when persistent attacks occur along that segment. In addition, data carrying certain labels may need to be prohibited from traveling over certain segments of the network. The selective routing feature enables these changes to be made in the routing of data across the network. Typically, the functionality of such a service is rated as none or present and the strength of the mechanism is given a rating between none and good. The Falcon LAN does not have this capability installed so the rating for the selective routing service would be none.

#### ***d. Summary of Falcon LAN Services***

Table 10 provides a rating summary of the services provided by the Falcon LAN. Various ratings may change as security features are added to the network. For example, if encryption software was implemented for all users, the ratings for non-repudiation, traffic flow confidentiality, and compromise protection could change. Since the network has not fully achieved the desired level of functionality, each of these services should be re-evaluated once all changes have been implemented.

| Network Security Service                       | Criterion                              | Falcon LAN Rating             |
|--|--|-------------------------------|
| Communications Integrity/<br>Authentication    | Functionality<br>Strength<br>Assurance | Present<br>Fair<br>Fair       |
| Communications Field<br>Integrity              | Functionality                          | None                          |
| Non-Repudiation                                | Functionality                          | None                          |
| Denial of Service/<br>Continuity of Operations | Functionality<br>Strength<br>Assurance | Minimum<br>Minimum<br>Minimum |
| Protocol Based Protection                      | Functionality<br>Strength<br>Assurance | Fair<br>Fair<br>Fair          |
| Network Management                             | Functionality<br>Strength<br>Assurance | Present<br>Fair<br>Fair       |
| Compromise Protection/<br>Data Confidentiality | Functionality                          | None                          |
| Traffic Flow<br>Confidentiality                | Functionality                          | None                          |
| Selective Routing                              | Functionality                          | None                          |

Table 10. Evaluation of Network Security Services for Falcon LAN

#### F. MEETING INTEROPERABILITY REQUIREMENTS

Ralph H. Sprague, Jr. and Barbara McNurlin define interoperability in their book Information Systems Management in Practice as "the capability for different machines, using different operating systems, on different networks to work together on tasks - exchanging information in standard ways without any changes in the command language or in functionality and without physical intervention." [Ref. 29: p. 186] Overall, achieving interoperability can be a quite cumbersome task and typically must

address both internal and external issues. Numerous aspects of the systems must be addressed, including policies, hardware, software, and protocols. Although many national and international committees have made progress over the years in developing standards aimed precisely at the interoperability issue, the end of the road has not yet been reached. In an era of piecemeal systems, a great deal of intervention is required to achieve total connectivity.

In meeting the interoperability requirements of the Falcon LAN, many issues needed to be addressed. As is typical with any LAN installation, the various functional requirements have been prioritized and are being implemented in their respective order of importance to the command. To date, not all requirements have been met. The following sections identify the interoperability issues that have been encountered thus far, and the status of each functional requirement.

#### **1. Provide a Communications System**

The primary goal of the LAN was to provide a backbone communication system for the various NSGD offices located in two different buildings. This was accomplished with the backbone installation conducted by NISE West and the subsequent computer installations conducted by the NSGD staff.

Since the software applications were all either Windows based (i.e., Microsoft) or Windows compatible, software interoperability within the LAN was not a major issue. There were, however, several problems due to the hardware configurations during the initial installation. For example, a CD-ROM drive was required for the



installation of Windows NT on the server. However, the CD-ROM drive purchased had an Integrated Drive Electronics (IDE) interface and NT requires a Small Computer Systems Interface-II (SCSI-II). Once a different CD-ROM drive was purchased and installed, it was not recognized by the hardware because of a SCSI adapter. The motherboard appeared to be confused between that and the SCSI adapter on the hard drive. The problem was solved once the adapter was removed from the CD-ROM drive. Additional problems arose from the amount of time (approximately one year) the hardware sat in storage prior to installation. For example, at least three of the ten mice did not work with the first set of computers installed. Eventually, the hardware problems were worked out and the staff had it's LAN.

## **2. Provide a Student Tracking System**

The development of a unified database for tracking student information was also desired. The database software selected for this task was Microsoft's Access and SQL server. Since SQL is part of the Microsoft Back Office suite, interoperability between the database software and the network operating system was not an issue. The actual development of the database is currently in progress.

## **3. Provide for Service Management**

Access was needed to the DLI Student Database, NITRAS, and the Army ATRRS programs to allow service needs and student eligibility requirements to be met. To date, access to the DLI database has not been achieved due to priorities assigned to the functional

requirements. Access to both NITRAS and ATRRS is being handled through dial-up access with a modem.

#### **4. Provide for Supply and Fiscal Tracking**

Access was also required to the Naval Postgraduate School supply system, the new supply and purchasing system, and on-line catalogs and supply status servers. This requirement is lower on the list of priorities than the DLI database. Therefore, it has not been accomplished to date.

#### **5. Provide Career Counseling Assistance**

This requirement was to provide for the maintenance and access to the student database with career counseling information such as ASVAB scores, next duty assignment, and prospective gains and losses. In addition, the Educational Services Officer requires access to course completion, PARS and other advancement information, and the staff required access to BUPER's bulletin boards and detailer E-mail.

The NSGD student database is currently being converted to Microsoft Access. Once the conversion is completed, it will then be formatted for the SQL server. Microsoft Access is a relational database management system which permits data to be viewed in various ways. The "Database Wizard" enables users to build tables, queries, forms, and reports from the data and the "Table Analyzer Wizard" enables data from flat-files and spreadsheets to be converted into a relational database. [Ref. 30] The SQL server provides the database management system functions needed for the distributed client-server environment.

The detailer electronic mail requirement has been achieved and is working smoothly. Access to BUPERS bulletin board is provided through two means: dial-up modem connectivity and the BUPERS World Wide Web (WWW) home page.

**6. Provide for Command Information Dissemination**

Dissemination and tracking of command welcome aboard packages, and access to NSGD home page from the World Wide Web (WWW) was required. These requirements have all been accomplished with WWW access provided through the DLI CISCO router. The NSGD home page can be found at <http://www.nsgdmry.navy.mil>.

**7. Allow for the Sharing of Electronic mail with DLI**

Access to and compatibility with the DLI Microsoft Mail server was needed to allow the transfer of electronic mail between the NSGD and DLI staffs. This included the requirement to establish electronic mail accounts for the NSGD staff and students. Electronic mail within the NSGD staff has been accomplished, however, connectivity with the DLI staff has not. Problems have been encountered due to the differences between the Microsoft Mail Server and Microsoft Exchange Server configurations. DLI will be changing from the Mail Server to an Exchange Server in the near future which should permit the connectivity to proceed. The fulfillment of this requirement remains in progress.

**8. Provide for the Instruction of the Cryptologic Technician Apprentice Common Core Curriculum**

Connections between the Falcon LAN and the new educational LAN in the Learning Center is desired. To date, this requirement has

not been fulfilled due to priorities and the need for hardware upgrades to complete the task. The hardware required for connecting the LANs has been received, just not installed.

**9. Provide for the Dissemination of Message Traffic on the LAN**

The ability to receive unclassified message traffic using the Defense Message System (DMS) was an additional requirement for the Falcon LAN. This is currently being handled through a stand-alone computer and was the focus of another thesis.



## VI. CONCLUSION - THE PRO'S AND CON'S OF ENSURING TRUST

*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*

- The Art of War  
Sun Tzu [Ref. 2: p. 207]

### A. CONCLUSIONS

| Requirement                       | Status  | Comments  |
|-----------------------------------|---------|---|
| Discretionary Access Control      | Met     |   |
| Object Reuse                      | Met     |   |
| Identification and Authentication | Not Met | Secure network interface needed; remote access may be a problem   |
| Audit                             | Not Met | Boot floppy vulnerability; Fortezza cards may take care of this problem   |
| Operational Assurance             | Met     |   |
| Life-Cycle Assurance              | Not Met | Testing is needed for a networked environment.  |
| Security Features User's Guide    | Met     |   |
| Trusted Facility Manual           | Met     |   |
| Test Documentation                | Not Met | Documentation based on a networked environment is needed.   |
| Design Documentation              | Met     | The Network System Architecture and Design need a thorough evaluation. However, this is listed as met because Windows NT is so thoroughly documented. |

Table 11. Analysis of Falcon LAN Class C2 Requirements

With the current configuration of the Falcon LAN, the system should not be accredited as providing a Class C2 level of trust. It does come close in many regards, although several requirements are met only in Windows NT in stand-alone mode. The issue of authentication is the major concern which needs to be addressed. Table 11 provides a breakdown of the TCSEC/TNI requirements for Class C2 and identifies the specific points of concern with respect to the Falcon LAN.

## **B. RECOMMENDATIONS**

After thoroughly evaluating the TCSEC and TNI criterion, there are two major recommendations for the Falcon LAN. First, the addition of secure network interface cards or Fortezza cards to the various components of the network may help to eliminate the authentication problems identified. NSA has expressed concern about the authentication problems of Windows NT and has agreed to pay for the development of a special version of the software which meets B-level requirements. Government Computer News announced in January that NSA had "awarded a contract to Global Internet of Palo Alto, California, to conduct a feasibility study on ways to beef up Windows NT 3.51 security and develop a prototype encryption card access control system based on Fortezza." [Ref. 31] If this upgrade does not come in time for meeting the Class C2 requirement, then depending upon the results of the current testing by the NCSC on Novell's Netware version 4.1, the command may want to investigate replacing the network operating system itself (Windows

NT Server) with Netware. Windows NT Workstation could still be maintained on the various components. However, prior to deciding on this course of action, research into the compatibility of the file systems (i.e., NTFS versus FAT tables) should be done to ensure a smooth transfer of files.

Netware 4.1 is being evaluated by the NCSC according to the TNI criterion and entered into the final evaluation phase in August 1995. The evaluation is covering "both the Netware 4.1 code and Cordant Incorporated's Assure bus-monitor card for ISA-bus systems and is designed to control user access to networks, peripherals, and local memory." [Ref. 32] Cordant is also working on a Fortezza integration with this card. If Netware 4.1 is certified, it will be the first network operating system to be certified for a network environment according to the TNI criterion.

Second, the incorporation of firewalls is recommended for helping to ensure the confidentiality of sensitive data. Threats from connecting to the Internet range from "curious prowlers to well-organized, technically-knowledgeable intruders that could gain access to a site's private information or interfere" with the availability of resources. [Ref. 32] During the past decade, firewalls have become a popular countermeasure to prevent unauthorized access from external sources.

A firewall is actually a collection of components used to protect one network from another untrusted network. Because the Internet is not secure and provides no performance guarantees, firewalls are typically thought of for accessing the Internet.



They can, however, be used between any two networks where one is not trusted. The purpose of the firewall is to provide controlled access to both internal and external services. Firewalls are important because they provide a single "choke point" where security and auditing features may be provided.

There are two types of firewalls: packet filtering gateways and application gateways. The packet filtering gateway operates at the Transport Layer of the TCP/IP architecture and simply blocks or filters traffic based upon the address and/or protocol. The application gateway operates at the Application Layer of the TCP/IP architecture, and provides a more specific level of filtering.

Packet filtering gateways are the easiest to configure and employ, but they are also the least effective. There is no logging capability on a packet filtering gateway, so it is difficult to detect if and when an intruder has corrupted the router. This type of firewall is also difficult to test for all vulnerabilities, because the firewall normally permits all traffic to pass unless specifically denied. If an intruder does break through the firewall, the host becomes directly accessible from the Internet. Finally, a firewall which depends solely on address filtering can be spoofed. "Spoofing is an attack in which a system attempts to illicitly impersonate another system by using its IP network address." [Ref. 34]

Application gateways are more secure, because they are application specific and have auditing capabilities. They are usually combined with a packet filtering gateway and add another

security filter at the application level. Consequently, an intruder's packet may pass through the initial packet filtering firewall, but it will not have direct access to the host system if it is also required to go through an application firewall. When the packet reaches the application gateway, the gateway checks its access matrices and grants or denies access to the requested application or service. If access is denied, the packets are logged and dropped. If access is granted, the packets are permitted access to the requested application, but nothing else. The application gateway never allows access to the host system and serves as a proxy for the requested service. It is very secure because it allows the network manager to control who has access to the network and its applications.

There is a false sense by many that a firewall is a security panacea for Internet security. A firewall, like any security countermeasure, is not the end all solution, but rather a tool to help safeguard system resources. The following security guidance is recommended with the use of firewalls on the Falcon LAN:

- Components which permit public access should be located outside of any firewalls. This would include dial-in modems and WWW servers.
- Install a packet filtering gateway to filter out unwanted guests based upon their address. Behind this firewall would reside all student and staff accounts with the data widely available. The firewall currently resident with the DLI CISCO router could be used for this requirement, but modem access behind the router (internal to the NSGD LAN) is discouraged. Modems provide a point of access to the LAN, which would circumvent the firewall.

- An application firewall behind the first firewall should be installed to separate all sensitive data (e.g., grades, clearance information, etc.) from the rest.

There is a wide range of firewall products available today with respect to both quality and strength. Routers with built-in packet filtering gateways start at approximately \$3,000. Most commercial firewall packages range from approximately \$10,000 to over \$250,000 in price. "Home-grown" firewalls can be built for considerably less money, however, building a firewall requires a significant amount of skill and knowledge of the TCP/IP architecture. Regardless of the type of firewall selected, it will require regular maintenance, installation of software patches and updates, and regular monitoring.

During the fall of 1995, the National Computer Security Association (NCSA) organized the Firewall Product Developers' Consortium (FWPD) to bring major vendors of firewall products together. "The purpose of the consortium was to decrease confusion about computer firewall products, enhance quality, provide a common terminology and testing methodology, and improve the ease-of-use and security of firewall products." [Ref. 35] By February 1996, the consortium had developed a baseline of functions that firewall products should offer and procedures to certify products according to performance criteria. The performance criteria used includes the "ability to handle 90% of security threats based on the likelihood of attack by hackers, ease of use by hackers, and how much harm could be done." [Ref. 36] Application-level firewalls, in particular, are tested against "approximately 120 types of

network attacks and must resist the most common and dangerous ones in order to earn the NCSA certification. The tests emphasize the success or failure of the firewall against intrusion attempts, not the methods by which such attempts are blocked." [Ref. 37] The testing process does not stop once a product is certified, rather products are retested at least once per quarter to address changing business needs and new security threats. The intent of the certification program is to provide users with a level of assurance that the firewall will provide the desired protection against existing and future threats. Participating vendors and products that have been certified can be found through the NCSA home page at <http://www.ncsa.com>. The page currently has 16 certified products listed including Borderware, CheckPoint Firewall-1, AltaVista, IBM's Secured Network Gateway, Eagle, SunScreen SPF-100, and Gauntlet Internet Firewall System. [Ref. 38]

### **C. ADVANTAGES AND DISADVANTAGES OF THE TCSEC**

Requiring specific levels of trust for the military computer systems has both its advantages and disadvantages. The major advantage is that criteria provide a common basis for discourse. If a specific level of trust (e.g., Class C2) is specified, then users are guaranteed a system with at least the features and assurances prescribed by the TCSEC. Without some well-defined criteria, the users are left to the mercy of the vendor's marketing departments.

Other major advantages include an increased level of awareness given to computer security, an overall higher level of assurance against major threats to most systems, and a range of more secure products available to DOD activities. As the National Research Council noted in 1991:

If one waits until a threat manifests through a successful attack, then significant damage can be done before an effective countermeasure can be developed and deployed. Therefore, countermeasure engineering must be based on speculation. Effort may be expended in countering attacks that are never attempted. The need to speculate and to budget resources for countermeasures also implies a need to understand what it is that should be protected and why. [Ref. 2: p. 157]

By requiring military organizations to ensure a specified level of trust for their operational environment, the safeguards will hopefully be in place when an attack is attempted. The control of information could be compared to the need for sea control. Numerous resources are devoted to ensuring the proper controls are in place at sea. If the same controls were not in place, the resultant costs would be too great once an attack had occurred. Yet when it comes to controlling our information, too many systems have been implemented with little or no regard for security until a compromise has occurred. By forcing users to evaluate security threats and countermeasures, the overall security of the system will increase.

On the other hand, requiring a specific level of trust is not free. The added life-cycle costs to maintain the system and monitor the security features are increased as the level of trust

increases. Personnel must be available, trained, and dedicated to their jobs to ensure the security features of the hardware and software are not bypassed. Audit logs in particular, require numerous manhours to review. In addition, the purchase price of "trusted systems" will tend to be higher.

Another disadvantage to requiring trusted systems is the lack of availability of trusted hardware and software. To have a system evaluated by the NCSC for a certain level of trust is expensive both in terms of time and financial support. Most evaluations require years to complete, and many vendors are reluctant to initiate an evaluation due to these costs. In addition, there is an overall lack of products certified to operate in a networked environment, which describes the majority of systems used by the military today. Until the benefits from having a product certified outweigh the costs, the availability of certified products will remain a problem for many organizations.

Finally, the certification and accreditation process can be quite cumbersome for most commands. The military does not currently have enough personnel adequately trained to conduct a thorough system certification and the requirements can be confusing. Although using a certified product assists with the overall procedure, it does not replace the requirement to thoroughly evaluate the system for its operational environment. Until more certified products are available and personnel receive the appropriate training, many commands will continue to struggle with the certification and accreditation process.

#### D. SUMMARY

This thesis set out to examine the current applicability of the Class C2 level of trust in a typical command environment using Windows NT. In meeting this objective, the certification and accreditation requirements had to be closely examined as well as the software and hardware of the environment selected. Although the commercial-off-the-shelf products are getting much closer to providing an avenue for achieving the desired level of trust, there is still much progress to be made. Perhaps in the future, system administrators will be able to walk into a computer store and purchase products which are appropriate for the security requirements of their operational environment. Use of these products will not eliminate the requirement for certification and accreditation, but will make the attainment of trusted systems possible. However, until that day arrives, caution must be given to the network configurations selected to meet a command's functional requirements. In the meantime, the widespread establishment of Class C2 systems throughout the military remains on the road ahead.

## LIST OF REFERENCES

1. Shaffer, Steven L. and Alan R. Simon. Network Security. Academic Press, Inc., Cambridge, Massachusetts, 1994.
2. Stallings, William. Network and Internetwork Security: Principles and Practice. Prentice Hall, Englewood Cliffs, New Jersey, 1995.
3. Russell, Deborah and G.T. Gangemi, Sr. Computer Security Basics. O'Reilly and Associates, Inc., Sebastopol, California, 1991.
4. Baker, Richard H. Network Security: How to Plan for it and Achieve It. McGraw-Hill, Inc., New York, 1995.
5. National Computer Security Center, "Department of Defense (DOD) Trusted Computer System Evaluation Criteria (TCSEC)," DOD 5200.28-STD, Library Number S225,711, December 1985.
6. Lee, Theodore M.P. "A Note on Compartmented Mode: To B2 or Not B2?" Proceedings 15th National Computer Security Conference, Baltimore, 1992, pp. 448-458.
7. National Computer Security Center, "Assessing Controlled Access Protection," NCSC-TG-028 Version-1, 25 May 1992.
8. Pfleeger, Charles P. Security in Computing. Prentice Hall, Englewood Cliffs, New Jersey, 1989.
9. Brinkley, Donald L. and Roger R. Schell. "Concepts and Terminology for Computer Security." May 1993.
10. Harrison, M.A., W.L. Ruzzo, and J.D. Ullman. "Protection in Operating Systems." Communications of the ACM. Association for Computing Machinery, August 1976, pp. 461-471.
11. National Computer Security Center, "A Guide to Understanding Discretionary Access Control in Trusted Systems," NCSC-TG-003, 30 September 1987.
12. National Computer Security Center, "Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-003-85, 25 June 1985.
13. National Computer Security Center, "Introduction to Certification and Accreditation," NCSC-TG-029 Version-1, January 1994.



14. Wood, Charles, and et al. Computer Security: A Comprehensive Controls Checklist. John Wiley and Sons, New York, 1987.
15. National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria," NCSC-TG-005, 31 July 1987.
16. Epstein, Jeremy and et al. "An Unusual B3-Compliant Discretionary Access Control Policy," Cordant, Inc., 1995.
17. National Computer Security Center, "Trusted Network Interpretation Environments Guideline," NCSC-TG-011, 1 August 1990.
18. National Security Agency, "Information System and Network Security Procedures for Service Cryptologic Elements," Supplement 1 to NSA/CSS Manual 130-1, Fort George G. Meade, Maryland, 1995.
19. "False Microsoft Claims Found on their NT Web Site." <http://netware.novell.com/discover/compete/inaccur.html>, July 1996.
20. "NSTL Software Digest: Ratings Report." Software Digest, November 1994.
21. National Computer Security Center, "Final Evaluation Report: Microsoft, Incorporated Windows NT Workstation and Server Version 3.5 with U.S. Service Pack 3," NCSC-FER-95/003, 14 February 1996.
22. Microsoft Windows NT 3.5 Guidelines for Security, Audit, and Control. Microsoft Press, Redmond, Washington, 1994.
23. Microsoft Windows NT 3.51 Resource Kit. Microsoft Press, Redmond, Washington, 1995.
24. Constance, Paul. "C2 Rating Aside, NT Isn't Secure." Government Computer News, September 4, 1995, p. 19.
25. Saltzer, Jerome and Michael D. Schroeder. "The Protection of Information in Computer Systems," Proceedings of the IEEE, September 1975.
26. National Computer Security Center, "Department of Defense Password Management Guideline," CSC-STD-002-85, 12 April 1985.

27. Minasi, Mark, et al. Mastering Windows NT Server 3.5, Sybex, San Francisco, 1995.
28. Feibel, Werner. Novell's Complete Encyclopedia of Networking. Novell Press, San Jose, California, 1995.
29. Sprague, Ralph H. and Barbara McNurlin. Information Systems Management in Practice. 3rd edition, Prentice Hall, 1993.
30. "Microsoft Access." <http://www.microsoft.com/products/access.html>, June 1996.
31. McCarthy, Shawn P. "NSA Will Pay for B-Level NT Development." Government Computer News, January 22, 1996, p. 6.
32. Olsen, Florence. "C2 Certification Close for Netware 4." Government Computer News, September 4, 1995, p. 8.
33. Chapman, Brent. "Building Internet Firewalls." <http://www.greatcircle.com/tutorials/bif.html>, August 1996.
34. Gilliland, Steve. "Moving to the Net? Think About Your Route." Data Based Advisor, v14, May 1996, p. 60.
35. "NCSA Establishes Firewall Product Developer's Consortium." The OSINetter Newsletter, v10, September 1995, p. 21.
36. Anthes, Gary H. "Firewall Chaos: Association Moves to Reduce Confusion in Turbulent Market." Computerworld, v30, February 5, 1996, p. 51.
37. Wilkerson, Robert. "NCSA Established Firewall Certification." PC Week, v13, March 11, 1996, p. N9.
38. "NCSA Firewall Certification Program." <http://www.ncsa.com/fpfs/fwindex.html>, August 1996.



## BIBLIOGRAPHY

- Amoroso, Edward. Fundamentals of Computer Security Technology. Prentice Hall, Englewood Cliffs, New Jersey, 1994.
- Cobb, Stephen. The Stephen Cobb Complete Book of PC and LAN Security. Windcrest Books, Blue Ridge Summit, Pennsylvania, 1992.
- Fisher, Sharon and Marcia A. Jacobs. "Microsoft, Novell Seek C2 Approval." Communications Week, September 4, 1995, p. 5.
- Fraser, B. Site Security Handbook (Draft). ftp://draft-ietf-ssh-handbook-03.txt, June 13, 1996.
- Hahn, Harley. The Internet Complete Reference. McGraw-Hill, Berkeley, California, 1996.
- Hughes, Larry J. Actually Useful Internet Security Techniques. New Riders Publishing, Indianapolis, Indiana, 1995.
- Icove, David, et al. Computer Crime: A Crimefighter's Handbook. O'Reilly and Associates, Inc., Sebastopol, California, 1995.
- Kaufman, Charlie, et al. Network Security: Private Communication in a Public World. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1995.
- National Computer Security Center, "A Guide to Understanding Configuration Management in Trusted Systems," NCSC-TG-006 Version-1, 28 March 1988.
- National Computer Security Center, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-004-85, 25 June 1985.
- National Computer Security Center, "Trusted Product Evaluation Questionnaire," NCSC-TG-019, 2 May 1992.
- Palmer, I.C. and G.A. Potter. Computer Security Risk Management. Van Nostrand Reinhold, New York, 1989.
- Schivley, Jody L. Network Security and the NPS Internet Firewall. Naval Postgraduate School Thesis, September 1994.

"Windows NT Platform Gets C2 Evaluation."  
<http://www.microsoft.com/NTWorkstation/c2.html>, June 1996.

### INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center ..... 2  
8725 John J. Kingman Road, Ste. 0944  
Ft. Belvoir, Virginia 22060-6218
2. Dudley Knox Library ..... 2  
Naval Postgraduate School  
411 Dyer Road  
Monterey, California 93943-5101
3. Naval Security Group Detachment, Monterey ..... 4  
Attn: CDR Gus Lott  
629A Rifle Range Road  
Monterey, California 93944-5005
4. Dr. Cynthia E. Irvine ..... 2  
Code CSIC  
Computer Science Department  
Naval Postgraduate School  
Monterey, California 93943-5118
5. Professor Rex Buddenberg ..... 1  
Code SM/Bu  
Department of Systems Management  
Naval Postgraduate School  
Monterey, California 93943-5118
6. Professor Roger Stemp ..... 1  
Code CS/Sp  
Computer Science Department  
Naval Postgraduate School  
Monterey, California 93943-5118
7. Fleet Information Warfare Center ..... 2  
Attn: LT Lucas  
2555 Amphibious Drive  
Norfolk, Virginia 23521-3225
8. Operations Systems Center ..... 1  
Attn: Deputy Director  
175 Murall Drive  
Martinsburg, West Virginia 25401
9. Commandant (G-SCT) ..... 1  
U.S. Coast Guard  
2100 2nd Street SW  
Washington, DC 20593-0001

10. Commandant (G-SCC) ..... 1  
U.S. Coast Guard  
2100 2nd Street SW  
Washington, DC 20593-0001
11. Commandant (G-SIA) ..... 1  
U.S. Coast Guard  
2100 2nd Street SW  
Washington, DC 20593-0001
12. Commandant (G-SII) ..... 1  
Attn: Harris McGarrah  
U.S. Coast Guard  
2100 2nd Street SW  
Washington, DC 20593-0001
13. Commandant (G-OP) ..... 1  
Attn: Capt. Richard Mead  
U.S. Coast Guard  
2100 2nd Street SW  
Washington, DC 20593-0001
14. Commander U.S. Coast Guard ..... 1  
TISCOM  
Attn: Bill Price  
7323 Telegraph Road  
Alexandria, Virginia 22304
15. Commander U.S. Coast Guard ..... 1  
TISCOM  
Attn: LCDR C. Johnson  
7323 Telegraph Road  
Alexandria, Virginia 22304
16. Commander U.S. Coast Guard ..... 1  
TISCOM  
Attn: Tom Clark  
7323 Telegraph Road  
Alexandria, Virginia 22304
17. Commander U.S. Coast Guard ..... 1  
TISCOM  
Attn: CWO Dykes  
7323 Telegraph Road  
Alexandria, Virginia 22304
18. Commanding Officer ..... 1  
USCG R&D Center  
1082 Shennecossett Road  
Groton, Connecticut 06304-6096

19. Commander, Naval Security Group Command ..... 2  
Code N9  
9800 Savage Road  
Ft. George Mead, Maryland 20755-6000
20. Commander, Naval Security Group Command ..... 2  
Code N61  
9800 Savage Road  
Ft. George Mead, Maryland 20755-6000
21. Dr. Blaine W. Burnham ..... 1  
R23  
National Security Agency  
9800 Savage Road  
Fort Meade, Maryland
22. Everett F. Batey ..... 1  
NSWSES  
2970 Luff Court  
Oxnard, California 93035
23. Rich Hale ..... 1  
Naval Research Laboratory  
Code 55  
4555 Overlook Avenue SW  
Washington DC, 20375